

IoTeX 2.0 – アクセス可能な DePIN!

バージョン **1.1** を更新しました

IoTeXチーム

2024年7月17日

抽象的な

分散型物理インフラストラクチャ ネットワーク (DePIN) は現在、Web3 で最も注目されているトピックの 1 つであり、近い将来に物理インフラストラクチャ ネットワークの構築、運用、管理方法を根本的に変える可能性のある大きなパラダイム シフトを表しています。資金と技術力の不足により、新興の DePIN スタートアップは、アイデアをタイムリーに市場に投入するという大きな課題に直面しています。このホワイトペーパーでは、IoTeX ネットワークの進化における変革的なステップである IoTeX 2.0 を紹介し、前述の課題に対処し、DePIN コミュニティが「DePIN for Everyone!」という究極のビジョンを実現できるようにすることを目指しています。

IoTeX 2.0 には、以下のコアイノベーションが含まれています。

- IOTXトークンの有用性を探求する新しいトークノミクス設計を検討します。包括的なモジュール式の DePIN インフラストラクチャ。
- DePIN スタートアップがコミュニティ所有の分散型インフラストラクチャ上にアプリケーションを構築できるようにするモジュール式 DePIN インフラストラクチャ。
- 統合された信頼できるレイヤーを提供するモジュラーセキュリティップール (MSP) 再ステーキングによるインフラストラクチャ モジュールの DePIN。

- W3bstream と呼ばれる分散型マルチ証明者ネットワークにより、DePIN ビルダーは
さまざまな有効性証明アプローチを活用して DePIN 検証を実現できます。
- DePIN アプリケーションでオンチェーン/オフチェーンのマシン対マシンおよびマシ
ン対人の関係を管理および保護する、ioID と呼ばれる統合 ID システム。
- ioConnect と呼ばれるユニバーサル組み込み SDK により、デバイスの抽象化が可能
になり、DePIN アプリケーションでのスマートデバイスのやり取りが容易になります。
- DePIN プロジェクトは、ioDDK によって自己主権型アプリケーションチェーンをプロビ
ジョニングし、IoTeX L1 のセキュリティを継承することができます。

目次

第1章 今日のDePIN	6
1.1 DePINが重要な理由	9
1.2 DePIN ステータス	10
1.3 DePIN技術スタックと課題	11
1.4 DePINのコンセプト	16
第2章 IoTeX 2.0	18
2.1 はじめに	18
2.2 私たちが作るもの(作らないもの)	22
2.3 Tokenomics	27
2.3.1 IoTeX 2.0 の IOTX ユーティリティ	28
2.3.2 インフレステーキング報酬	33
2.3.3 デフレ燃焼	35
2.3.4 成長インセンティブ	37
2.4 公共財	38
2.5 プロジェクトライフサイクル全体を通じてビルダーをサポートする	41
2.6 将来	42
第3章 モジュラー セキュリティプール (MSP) - DePIN インフラストラクチャ モジュール用の統合信頼層	45
3.1 問題	45
3.2 安全と信頼のためのオープンマーケット	46
3.3 アーキテクチャ	48
第4章 W3bstream - DePIN 検証のための分散型マルチ証明者ネットワーク	52
4.1 W3bstream アーキテクチャ	52
4.1.1 4種類の証明者	53
4.1.2 ZKPに関する社内イノベーション	58
4.2 W3bstreamワークフロー	59
4.2.1 証明者のオンボーディングと管理	59
4.2.2 ワークフロー	59
4.3 DePIN検証とオフチェーンAI	61
4.3.1 DePIN認証	61
4.3.2 オフチェーンAI	62
第5章 iold - DePIN 用の統一 ID システム	63
5.1 オンチェーンとオフチェーンのアイデンティティ	63
5.1.1 オンチェーンアイデンティティ	63
5.1.2 オフチェーンアイデンティティ	64
5.2 ioldの設計	65

5.2.1 デバイス上でのioID生成	66
5.2.2 デバイス上でのioID生成	67
5.2.3 安全なマシン間インタラクション	69
5.3 DePINプロジェクトへのioIDの統合	69
5.3.1 ioIDのスマートコントラクト 5	70
5.3.2 デバイスNFTコントラクトの展開	71
5.3.3 DePINプロジェクトの登録	71
5.3.4 デバイスNFT契約の設定	72
5.3.5 ioIDのリクエスト	72
5.3.6 デバイスの登録	72
第6章 ioConnect - デバイスの抽象化を強化するためのユニバーサル組み込み SDK	73
6.1 接続オプション	74
6.1.1 集中接続レイヤーへの接続	74
6.1.2 分散接続層への接続	75
6.2 DePINデバイス用のユニバーサル組み込みSDKを構築するための設計上の考慮事項	76
6.2.1 Arm の PSA 認定暗号 API	77
6.2.2 自己主権アイデンティティ(SSI)	78
6.3 実装仕様	78
6.3.1 ioConnect SDK コア	79
6.3.2 DePINデバイスの互換性	80
第7章 ioDDK - 自己主権型 DePIN アプリ チェーンの有効化	81
7.1 設計の根拠	81
7.2 共有ブロックスペースとバリデーター	83
7.3 ioDDK コンポーネントと高レベルワークフロー	85
7.3.1 ioDDK コンポーネント	85
7.3.2 高レベルワークフロー	86
7.4 ブロックスペースをレンタルするためのマーケットプレイス	87
7.5 IoTeX L1への影響	88
第8章 新しいロードマップ	91
第9章 結論	92

第1章

今日のDePIN

IoTeXは、2017年に設立され、モノのインターネット(IoT)をブロックチェーンに接続することで、人々がスマートデバイスを所有および制御し、デバイスが生成するデータと価値を制御できるようにしています。IoTeXの設立のテーマは、分散型ブロックチェーンを使用して数十億のスマートデバイスをオーケストレーションすることで、信頼性、セキュリティ、相互運用性など、既存のモノのインターネットの主要な問題が解決され、ユーザー所有のデバイスネットワークが繁栄するための新しいパラダイムが実現することです。過去6年間、IoTeXは現実世界とブロックチェーンの統合を先導し、いくつかのコアユースケースを調査および構築してきました。

- **マイクロペイメント(2017-2018)**: ブロックチェーンをグローバルなデジタル決済レイヤーとして活用し、デバイス、機械、ネットワーク間の自動化された安価な支払いを推進します。そして個人。ブロックチェーンは、これまで統合されていませんでした。相互運用可能なデバイスは、通信および取引を行うために使用されます。
- **出所とサプライチェーン(2018-2020)**: ブロックチェーンを信頼のない会計および所有権台帳として活用し、スマートデバイスや分散型サプライチェーンのユースケース(例:Pebble Tracker [1,2])の出所を可能にします。チェーンは信頼できるデバイスからデータを収集し、現実世界のアクティビティを検証し、新しいイベントやワークフローをトリガーします。
- **データの所有権とプライバシー(2020~2021年)**: ブロックチェーンを分散型アイデンティティレイヤーとして使用し、エンドツーエンドの暗号化、マルチパーティコン

ピューティング、機密コンピューティングなどの高度な暗号化を組み込んで、人々が自分のデバイスとデータを所有および制御できるようにします(例:Ucam [3,6])。

Arm [7, 8]などの大手企業と提携して開発された分散型プライバシーソリューション。

- **DePIN (2021-現在):** ブロックチェーンを分散型物理インフラストラクチャ ネットワーク (DePIN) の基盤として使用します。これは、人々が現実世界のインフラストラクチャ ネットワークに貢献し、公平性を構築できるようにする、資本形成と人的調整のための新しいモデルです。De-PIN が生成するデータとサービスは、他のユースケース カテゴリ、つまり人工知能 (AI) や現実世界資産 (RWA) への入力としても機能する可能性があります。

2017年に発行されたオリジナルのIoTeXホワイトペーパー[5]では、IoTeXプラットフォームは、接続方法の基本的な理解を提供します •データの所有権とプライバシー (2020-2021年): ブロックチェーンを分散型アイデンティティレイヤーとして使用し、人々が自分のデバイスを所有し、制御できるようにします。安全でスケーラブル、多目的かつ分散化されたL1は、プライバシー保護技術とデバイス指向のミドルウェアを組み込んでおり、物理的な接続を実現します。そしてデジタルの世界。長年にわたり、私たちは多くの野心的な目標を実現してきました 現実世界をブロックチェーンに安全に統合する。当初のホワイトペーパーで達成しようとした目標は次のとおりです。

- IoTeX メインネットは、ダントンタイムやハッキングなしで約 1 億 2,000 万件のトランザクションを処理しました。
- 最初のブロックチェーン互換ハードウェア デバイス (Ucam や Pebble Tracker など) は、ビルダー向けのすぐに使えるハードウェア開発キットとして IoTeX によって設計および製造されました。

- サードパーティのさまざまなスマートデバイスが IoTeX プラットフォームに統合されており、現実世界をブロックチェーンに安全に接続する方法についての基本的な理解を提供します。
- DePIN プロジェクトのエコシステム全体が、スマートデバイスからの実世界データを組み込んだ IoTeX 上で開始されました。
- IoTeX ネットワークの生命線となるネットワーク検証者、開発者、ユーザーのグローバルコミュニティが設立されました。

しかし、これはほんの始まりに過ぎません。ブロックチェーンの世界は2017年以降飛躍的に成長しており、De-PINが広く普及するためには何が必要かをより深く理解できるようになります。IoTeXコア開発者は、IoTeXのビジョン構築と並行して、ゼロ知識証明、オフチェーンスケーリング、デバイスの自己主権型ID、DePINセクター全体を前進させる公共財など、DePINを次のレベルに引き上げる新しいイノベーションの研究と設計に取り組んできました。私たちが導入する IoTeX 2.0ビジョンは、IoTeXネットワークを拡張するための3年間の計画を概説しています。私たちは、新しいモジュール式プラットフォーム設計を組み込み、トークノミクスを更新するなど、DePINスペースやその他のビルダーの高まる需要を満たすことを目指しています。この更新されたビジョンにより、私たちはついに「DePINをすべての人間に」という究極の目標を実現することができます。

1.1 DePINが重要な理由

IoTeX 2.0 と DePIN の将来ビジョンについて詳しく説明する前に、まず DePIN とは何か、そしてなぜ気にする必要があるのかをお話ししたいと思います。今日、通信、エネルギー、コンピューティングなど、世界で最も重要な産業や公共事業の多くは、中央集権的な企業や政府によって所有および管理されている独占や寡占です。これらの 1 兆ドル規模の産業は、財務的にもロジスティック的にも非常に高い参入障壁を備えています。たとえば、AT&T

は年間 240 億ドルを費やし、通信帝国を運営するために 16 万人以上の従業員を必要としています。これらの巨大な参入 障壁のため、一般の人々が選択できる商品やサービスのプロバイダーはわずかしかありません。つまり、競争は制限され、イノベーションは抑制され、消費者は他に選択肢がないため、標準以下の顧客サービスと過度に高騰した価格に耐えなければなりません。巨大企業は、何百万人もの顧客にサービスを提供すると同時に、自分たちの利益のために人々から機密性の高い貴重なデータを密かに抽出している。そこから生じる問題はさらに深刻である。新興市場国では顕著であり、富の格差がさらに深まり、一般の人々の機会が制限されています。

DePIN は現状を変える革命的な概念です。オープンソースの分散型ブロックチェーン上に構築された DePIN は、低コストまたは無償で世界中の何十億もの人々にサービスを提供する物理的なインフラストラクチャと公共施設に透明性、信頼性、革新をもたらすことができます。しかし、今日の世界を修正することは、DePIN の真の可能性のほんの一部にすぎません。本当のチャンスは、現在の世界の問題を単に修正することではなく、一般の人々が所有、運営、利用する公共施設を備えた新しい世界を構築することです。DePIN により、誰もが現実世界のインフラストラクチャ ネットワークに貢献し、株式を構築できるようになり、前述の財務的およびロジスティックスの参入障壁を克服できます。分散型金融 (DeFi) によって普及した新しい資本形成方法を利用してネットワークリソースをクラウドソーシングすることで、DePIN はユーザーが提供したハードウェア、人材、地域の専門知識を集約して新しいインフラストラクチャ ネットワークの構築を推進し、貢献者に作成を支援したネットワークの株式で報酬を与えることができます。最後に、DePIN はブロックチェーン上の不変のスマートコントラクトを活用して、ネットワークにとって最善となるように貢献者の行動を検証および調整できます。

DePIN は、現在の世界を改善する道筋を提供するだけでなく、より良い世界を設計する機会も 提供します。私たちは、化石燃料や有線インターネットなどの数十年前のインフラストラ

クチャが、再生可能エネルギー やワイヤレスなどの革新的なインフラストラクチャに置き換えられる新しい産業革命の瀬戸際にいます。DePINを使用すると、誰もがグローバルインフラストラクチャの近代化に貢献し、このインフラストラクチャが表す数兆ドルの価値の公平な分け前を受け取ることができます。人々による、人々のための新しい世界 - それが DePIN の約束です。DePIN はすべての人のためのものです

1.2 DePIN ステータス

DePINは、世界中の数百のプロジェクトによる共同取り組みであり、すべての物理的なインフラストラクチャの分散化と改善を目指しています。用語「DePIN」は2023年に生まれましたが、DePINセクターは2017年からIoTeX、Helium、Filecoinなどのプロジェクトが先駆者として活躍しており、それよりずっと前から活動しています。現在、DePINの状況は多様であり、DePIN固有のインフラストラクチャを構築するプロジェクトと、複数の垂直分野にわたるDePINアプリケーションで構成されています。DePINは現在、ブロックチェーンの最も有望なユースケースの1つであり、物理リソースネットワークとデジタルリソースネットワークに細分化できます。これらは、ネットワークが提供するサービスの種類によって指定されます。物理リソースネットワークは、本質的により具体的な非代替リソース(つまり、どのデバイスからのデータ/サービスも一意)を生み出し、一般的に場所に依存するハードウェアに依存します。一方、デジタルリソースネットワークは、本質的により仮想的で、場所に依存しないハードウェアに依存する代替リソース(つまり、1GBのストレージは1GBのストレージ)のマーケットプレイスを生み出します。DePINセクターには、カテゴリの成長を促進し、DePINアプリケーションにすぐに使用できる機能を提供するインフラストラクチャとツールも含まれます。包括的なDePINランドスケープを図1.1に示します。

1.3 DePIN技術スタックと課題

DePINは、現実世界とブロックチェーン世界を接続するエンドツーエンドの技術スタックが必要です。NFTなどのデジタル資産やステーブルコインなどの金融資産の交換を容易にするブロックチェーンのユースケースとは異なり、DePINは膨大な量のデータを生成する現実世界のスマートデバイスとインターフェイスする必要があります。ブロックチェーンは不変の台帳として、現実世界で何が起こったかの事実を文書化するのに最適な基盤です。ただし、デバイスからブロックチェーンに「現実世界の活動の証明」を永続的に書き込む前に、現実世界の活動が実際に起こったこととデータが信頼できることを確認するための一連の手順を完了する必要があります。デバイスはオンチェーンで登録され、生のデータが収集、解析、保存され、データに対する計算が検証可能な方法で実行されて初めて、「現実世界の活動の証明」がブロックチェーンに決済されます。

DePIN ランドスケープ

JUL 2024 分散型物理インフラストラクチャネットワーク

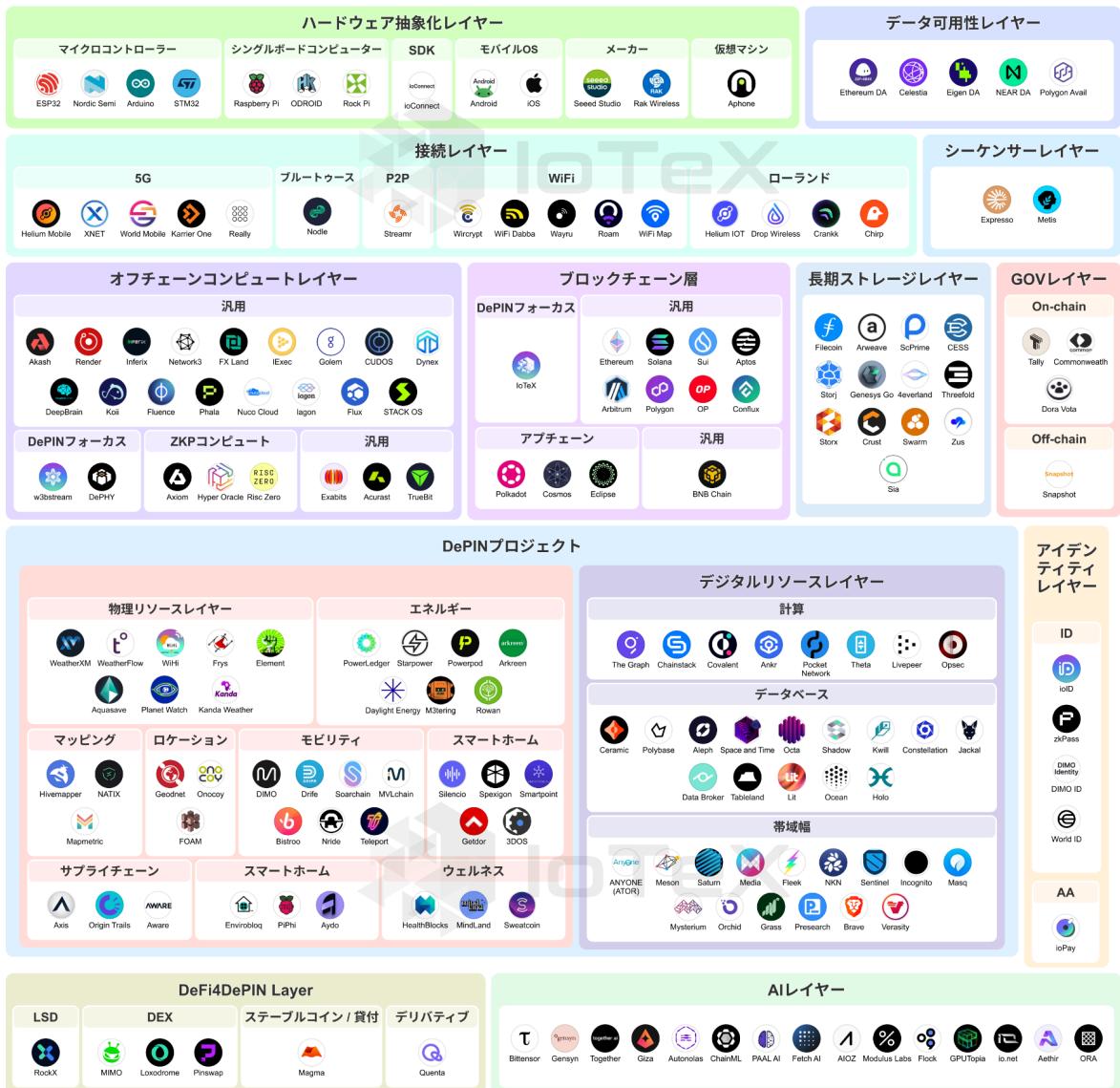


図 1.1: DePIN の状況

図1.2に示されているように、DePINプロジェクトで考慮すべき9つの重要なレイヤーを紹介します。

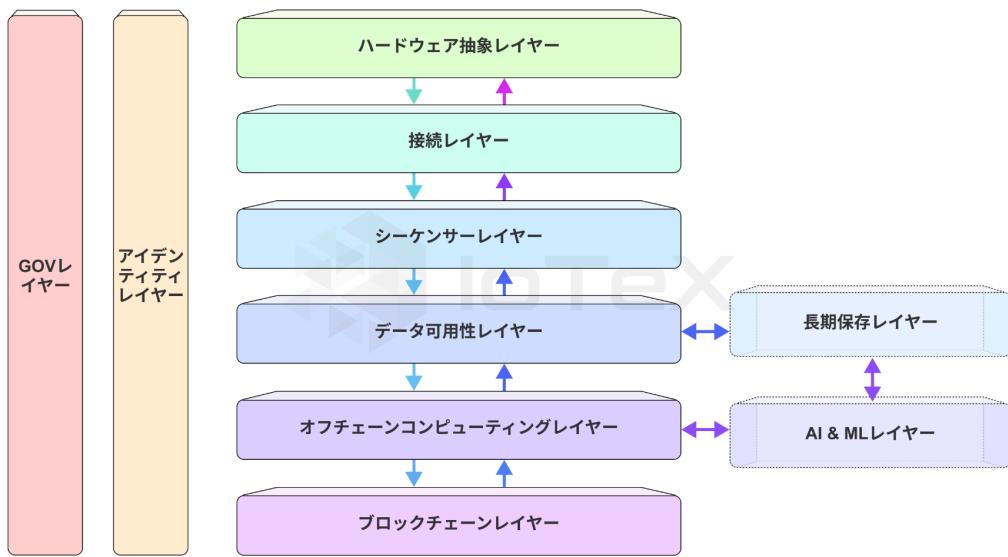


図 1.2: DePIN 技術スタック

- ハードウェア抽象化レイヤー:大型から小型まで幅広いスマートデバイスが接続レイヤー内のエンティティと安全に接続できるようにします。
- 接続層:スマートデバイスによって生成されたデータを確実に中継し、シーケンサー層
- シーケンサー層:スマートデバイスからのデータパケットをデータ可用性層に送信する前に順序付けます
- データ可用性レイヤー:即時使用とセキュリティ検証のためにデータを保存し、オフチェーンデバイスが情報にアクセスして生データから洞察を生成できるようにします。
- 長期保存レイヤー:生データと洞察をアーカイブし、将来の使用に備えて、コンプライアンス、分析、AIなど。

- オフチェーンコンピューティングレイヤー:データ可用性レイヤーに保存されたデータにビジネスロジックを適用し、現実世界の活動に関連する洞察と証明を生成します。
- ブロックチェーンレイヤー:デバイスのIDとデータの信頼アンカーとして機能し、オフチェーン計算の有効性を検証し、DePINの利害関係者にトーカン報酬を配布します。
- アイデンティティレイヤー:関係するすべてのエンティティ(スマートデバイス、ユーザー、サーバー、メーカー、バリデーターなど)のオンチェーンおよび/またはオフチェーンのアイデンティティを管理します。
- ガバナンス層:通常はコミュニティ投票制度を通じて、分散型の方法でネットワークボリシーと手順(インセンティブなど)を実施します。

DePINの技術スタックの広範なレイヤーは、単一のチームがモノリシックな方法で開発するには手に負えない可能性があります。この複雑さにより、開発者がDePINで革新的なアイデアを試すための参入障壁が高くなります。過去数年間、資金力のあるプロジェクトは、多額のベンチャー キャピタルを調達し、独自のモノリシックな技術スタックを開発することで、これらの課題を克服してきました。ただし、DePINが真に繁栄し、世界中の隅々(ラテンアメリカ、アフリカ、東南アジアなど)に到達するには、大規模な技術スタックと高度な技術の複雑さにより、次のような追加の課題が生じます。

- 発売速度: DePINが初期需要を促進するための供給の最小しきい値に達する速度は、ハードウェアの制約と先行資本支出要件により制限されます。

- 需要側の成長: DePIN は、供給をブートストラップするまでの長い道のりと、ユーザー エクスペリエンス、信頼性、コストに関して既存のソリューションと同等を達成することが難しいため、需要の構築に苦労しています。
- トークンの流動性: DePIN はトークンのインセンティブを使用してネットワークの成長を促進し、インフラストラクチャの運用に資金を提供しますが、プライホイールを閉じてチェーン上の流動性を構築するのに苦労しています。
- 認知度: DePIN は特定の業界に焦点を当てることが多く、特に業界に直接関与していない人にとっては、プロジェクトの目的や成功の指標が必ずしも明らかではありません。

これらの課題により、DePIN はまだかなり初期段階にあり、市場価値と採用の点で DeFi や他の暗号セクターをまだ上回っていません。DeFi と DePIN は多くの点で似ていますが、最も顕著なのは、人々（「供給側」）からリソースをクラウドソーシングして、他の人々が望み、使用する製品（「需要側」）を作成することです。ただし、需要と供給を獲得して維持するための方法は、DeFi と DePIN では大きく異なります。大まかに言えば、DeFi の需要と供給はブートストラップが容易ですが、一時的なものです。一方、DePIN の需要と供給はブートストラップが難しいですが、時の試練に耐える能力があります。さらに、DePIN は、少量の集約された資金がすぐに需要を生み出す可能性がある DeFi とは異なり、初期需要を生み出すために大量のリソースを集約しなければならないことがよくあります。上記の課題に対して DePIN と DeFi を並べて比較すると、図 1.3 に示すように、次の詳細な違いがわかります。

1.4 DePINのコンセプト

我々は、DePINがすべてのビルダー、すべての貢献者、すべてのユーザーのためにあると強く信じています。この信念は、次の点を強調しています。

- 小規模チームや個人開発者でも、重要なシステムを構築できます。DePIN 製品は、最高水準のクラスインフラストラクチャを利用しています。
- DePINプロジェクトは、高額な初期費用をかけずに迅速に反復できる必要があります。真の革新を見極める。
- DePIN のプロジェクトは、機能 (たとえば、個人の指輪、車、電話からのデータの集約) と地域 (Uber の 都市別モデルなど) の両方の観点から構成可能である必要があります。
- ネットワークに価値や有用性を提供するネットワーク貢献者には、参入障壁が低く、安定的かつ長期的に金銭的な報酬が与えられるべきです。
- ユーザーは、公共の革新的な公共サービスに公平にアクセスできるようになるべきであるこれらの DePIN ネットワークから。

この信念は単なる希望的観測ではありません。以下に示すように、IoTeX 2.0 として知られる技術設計に実際に反映されています。

	DeFi	DePIN	DePINの挑戦	部分解決策
技術スタック	シンプルかつデジタルのみ: 例: 主に Solidity + JS、フォークして起動するのが簡単	複雑で物理世界と関わる。C/C++、Golang/Python/Rust、Solidity、JS、そしてオプションでSwiftを使い、フォークするのが難しい。	課題1: DePIN プロジェクトは、ハードウェア コンポーネントが原因で構築が難しく、立ち上げに多くの資本が必要になります。探索は遅く、費用がかかります。	<ul style="list-style-type: none"> プロジェクトを中央集権方式で立ち上げ、市場を「テスト」し、意思決定を加速させる 分散化と信頼性の欠如が、貢献者と投資家を躊躇させる可能性がある
発射速度	速い: 例: dAppをグローバルにローンチ; 少数の“大型”資本を持つ“マイナー”が供給サイドをすばやくセットアップ	遅い: 例: プロジェクト固有のハードウェアの出荷と展開、ネットワークが必要に対応できる供給のしきい値スケールが高い可能性がある。	課題2: DePIN プロジェクトは、ハードウェア制約により立ち上げ（供給側を確立）が遅いため、暗号化サイクルとの不一致が生じる可能性があります。	<ul style="list-style-type: none"> T-Mobileのような既存のWeb2パートナーと連携し、より早くしきい値規模に到達する Web2パートナーが存在しない革新的なDePINネットワークには適用されない
需要側の成長	適切に設計すればユーザーを引き付けやすい、例: イールドファーミング、しかし通常は短期間	セルラープランの顧客に加入するなど、ブーストストラップには時間がかかりますが、長期的には影響力が大きくなる可能性があります。	課題3: 暗号通貨は不需要に複雑なUXを提供し、デマンドサイドの導入を遅らせる可能性がある。	<ul style="list-style-type: none"> トークンを使って一般の人々にDePINを採用し、利用してもらう ほとんどの人が暗号通貨ネイティブではなく、トークン、ウォレットなどを理解していない
トークンの流動性	トークンの流動性は取得しやすく、金融アプリケーションの自然な副産物	創設者や貢献者は財務経験よりもハードウェアや Web2 の経験が豊富であるため、トークンの流動性を達成するのが難しいことがあります。	課題4: トークン流動性は、すべての暗号プロジェクトにとって重要ですが、トークンインセンティブでネットワークの成長を促進する DePIN にとって特に重要です。	<ul style="list-style-type: none"> DePINチームは、CEXとマーケットメーカーと協力して、トークンの流動性を獲得できる これは高価で長期的なプロセスとなる可能性がある
シェアリングネットワークの拡大	成功の指標が明確、例: TVL、取得と表示が容易	成功の指標はプロジェクト固有であり、物理デバイスから取得する必要があります	課題5: ブロックチェーンレイヤー	<ul style="list-style-type: none"> オンチェーンデータは、Duneのようなツールを使って比較的簡単に取得し、表示できる しかし、多くのDePINは非常に中央集権的に開始され、表示できるオンチェーンデータがあまりない

図1.3: DePINとDeFiの比較

第2章

IoTeX 2.0

2.1 はじめに

IoTeX 2.0 は、今後数年間の IoTeX ネットワークの壮大なビジョンとロードマップを定義し、「すべての人のための DePIN」を実現するという当社の使命を拡大し、DePIN 業界のパイオニアとしての長年の経験から生まれたものです。当社の目標は、DePIN プロジェクトが現在直面している技術的および非技術的な課題に対処するだけでなく、IoTeX を世界最大の DePIN エコシステムにすることで、将来の DePIN の可能性を最大限に引き出すことです。これを実現するために、私たちは IoTeX 2.0 を発表できることを嬉しく思います。IoTeX 2.0 は、新しい哲学、テクノロジー、トークノミクス、公共財、イニシアチブを組み合わせて、一般の人々が DePIN に貢献できるようにし、ビルダーが現実世界とブロックチェーンの世界を真に橋渡しできるようにします。

IoTeX 2.0 では、IoTeX ネットワークは単なる L1 ブロックチェーンから、IOTX トーカンを介して固定されるオープン DePIN インフラストラクチャ、Dapps、および L2 に進化します。これにより、IoTeX ネットワークへの参加者や貢献者の数と種類が大幅に増加し、最終的には IoTeX と DePIN の範囲が新たな領域に拡大されます。DePIN は誰にとっても有益であるべきであり、それが IoTeX の理由です

2.0 では、ライフサイクルのあらゆる段階で構築者とユーザーを含めることが優先されます。確立された Dapp であっても、独自の L2 への拡張を希望しているかどうか IoTeX 2.0 は、

DePIN ベースのビジネス モデルの実装を目指す従来の企業、または大きなアイデアを持つ小規模なチームに対して、すべての DePIN ビルダーに関連する完全な機能スイートを提供します。

私たちの中心的な方法論は、モジュール式 DePIN インフラストラクチャです。DePIN プロジェクトは、モジュール式サービスのメニューから選択することで、特定の段階と要件に適した技術スタックを構築できます。これらの製品には、IoTeX coredev によって構築された社内製品と、トップ プロジェクトのパートナー製品が含まれます。モジュール式アプローチの主な利点は、インフラストラクチャ構築者が最も得意とする機能に集中し、共通の目標を達成するために協力できることです。当社のモジュラー製品には、オーフェーンスケーリング、ゼロ知識証明、人工知能などの最先端のテクノロジーが組み込まれており、DePIN セクターに独自のイノベーションをもたらします。これらのモジュールは、IoTeX coredev だけでなく、専門のインフラストラクチャビルダーによっても構築されており、IoTeX を使用してセキュリティと信頼性を確保しています。このアプローチは、最大規模の DePIN チームに包括的なソリューションを提供すると同時に、新しい DePIN プロジェクトを迅速かつ安全に作成するために使用できる小規模なチーム専用のソリューションも提供します。

アーキテクチャの観点から見ると、IoTeX 2.0 は次の観点を重視しています (図 2.1 を参考)。

- **モジュラー セキュリティプール (MSP):** モジュール性の基盤は、IOTX およびその他の主流の資産によってサポートされている、統合された信頼できるレイヤーであり、これを MSP と呼びます。これらは、IoTeX L1 に展開された一連のスマートコントラクトです。IoTeX L1 と MSP はどちらも、DePIN インフラストラクチャ モジュール (DIM) レイヤーと Dapp/L2 レイヤー内のすべてのアクティビティの信頼アンカーおよび変更

不可能な台帳として機能します。大まかに言えば、MSPにより、IoTeX L1 は DePIN 技術スタックのさまざまな部分にまたがる DIM にプルーフオブステークセキュリティを提供できます。DIM プロバイダーは、IOTX およびその他の主流の資産をステークして MSP に参加します。さらに、MSP からセキュリティと信頼を獲得した DIM は、その状態を IoTeX L1 に断続的に固定し、dApp ビルダーが信頼できる現実世界のアクティビティに基づいて革新する可能性を開きます。

- **DePIN インフラストラクチャ モジュール (DIM):** IoTeX 2.0 の新しい DIM レイヤーは、DePIN 技術スタック全体を網羅するモジュール式の機能セットを提供します。世界的なビルダーからの貢献を促進しながら、IoTeX コア開発者はいくつかのレイヤーの社内実装を提供します。AI 推論、ストレージ、プライバシー保護コンピューティング、データ分析、RPC、ドメイン名システムなどの追加の DIM は、IOTX を MSP にステークするパートナーやビルダーによって提供されます。必要に応じて、各 DIM が独自のトークンを持つことができることに注意してください。
- **公共財:** IoTeX の目標は、DePIN を新しい領域に導くことです。そのためには、誰もが信頼でき、自由に利用できる公共財が必要です。私たちの目標は、開発者がシームレスに統合し、ユーザーに提供してオープンな参加を促進できるオープンソースリソースのスイートを作成することで、DePIN ムーブメントをリードすることでです。これらの公共財には、ユーザー向けツール（エクスプローラー、ウォレット、ブリッジなど）、開発者向けツール（IDE など）、ネットワーク全体のリソース（ガバナンス、資金など）が含まれます。
- **実力主義トークノミクス:** IoTeX ネットワークに新しいレイヤーが追加されると、新しいステークホルダーが加わり、さまざまなカテゴリにわたって専門知識を提供します。刷新されたトークノミクスの目標は、IOTX トークンの実用性を拡大するだけでなく、ス

テークホルダーの貢献度に基づいて報酬が分配される実力主義の方法で拡大することです。IoTeX ネットワークの範囲が拡大すると、IOTX トーカンに新しい実用性がもたらされ、DePIN セクターの基盤となる通貨になります。

- **DePIN Dapps と DePIN L2s:** テクノロジー スタックの最上位には、IoTeX 2.0 の DIM の一部またはすべてを活用する DePIN Dapps と L2s のエコシステムがあります。多くの Dapps は IoTeX L1 でネイティブ トーカンを起動し、すべての DIM オファーリングを活用することを選択しますが、一部の Dapps は 1 つまたは複数の DIM のみを利用することを選択する場合があります。IoTeX 2.0 のモジュール重視により、Dapps は現在の状態のニーズに基づいてさまざまなモジュールを活用しながら、将来のニーズに合わせて新しい機能を利用できるようになります。さらに、DIM レイヤーの新しいコンポーネントは ioDDK です。これは、プロジェクトが IoTeX L1 上に独自の L2 を起動できるようにする L2 チェーン SDK です。これにより、DePIN は独自の主権トーカン経済圏を構築し、独自の Dapps をホストできるようになると同時に、DIM レイヤーの幅広い機能の恩恵を受け、IoTeX L1 からのセキュリティと信頼を獲得できるようになります。

2.2 私たちが作るもの(作らないもの)

セクション 1.3 で述べたように、DePIN を構築するには、幅広い機能を網羅する多層技術スタック (図 2.2 を参照) が必要です。IoTeX 2.0 で新しく導入された DIM レイヤーは、これらの技術スタックの各要素に対するソリューションを提供します。この DIM レイヤーは完全にオープンであり、インフラストラクチャビルダーは実装を組み込むことができます。これにより、DePIN プロジェクトは、カスタム技術スタックを作成するための幅広いオプションを利用できるようになります。

IoTeX コア開発者が内部で開発したコア モジュールに加え、特殊な機能を備えたブロックチェーン分野の主要プロジェクトから多数のモジュールが提供されます。たとえば、データ可用性レイヤーは Celestia や NEAR などのプロジェクトの主な焦点であり、長期ストレージレイヤーは Filecoin や Arweave などのプロジェクトの中心です。IoTeX 2.0 はモジュール性と構成可能性を重視しているため、すべてのプロジェクトを DIM レイヤーに統合し、DePIN プロジェクトが好みの技術スタックを設計できるようにしています。

当社は DIM レイヤーのあらゆる部分への提供を歓迎していますが、IoTeX コア開発者は、DIM、ハードウェア、ID、オフチェーンコンピューティング、L2 SDK、公共財の統合された信頼できるレイヤーに重点を置いたいくつかの重要なモジュール向けの最先端のソリューションを研究および開発しており、以下で概要を説明し、次のセクションで詳細に検討します。

- **MSP (DIM 向け統合信頼レイヤー):**これは、IoTeX L1 上の一連のスマートコントラクトで構成された統合信頼レイヤーです。ステークされた IOTX やその他の主流の資産を取得し、そのセキュリティを他の DIM に貸し出します。
- **W3bstream (オフチェーンコンピューティングDIM):**社内およびサードパーティの分散型オフチェーンコンピューティングネットワーク。

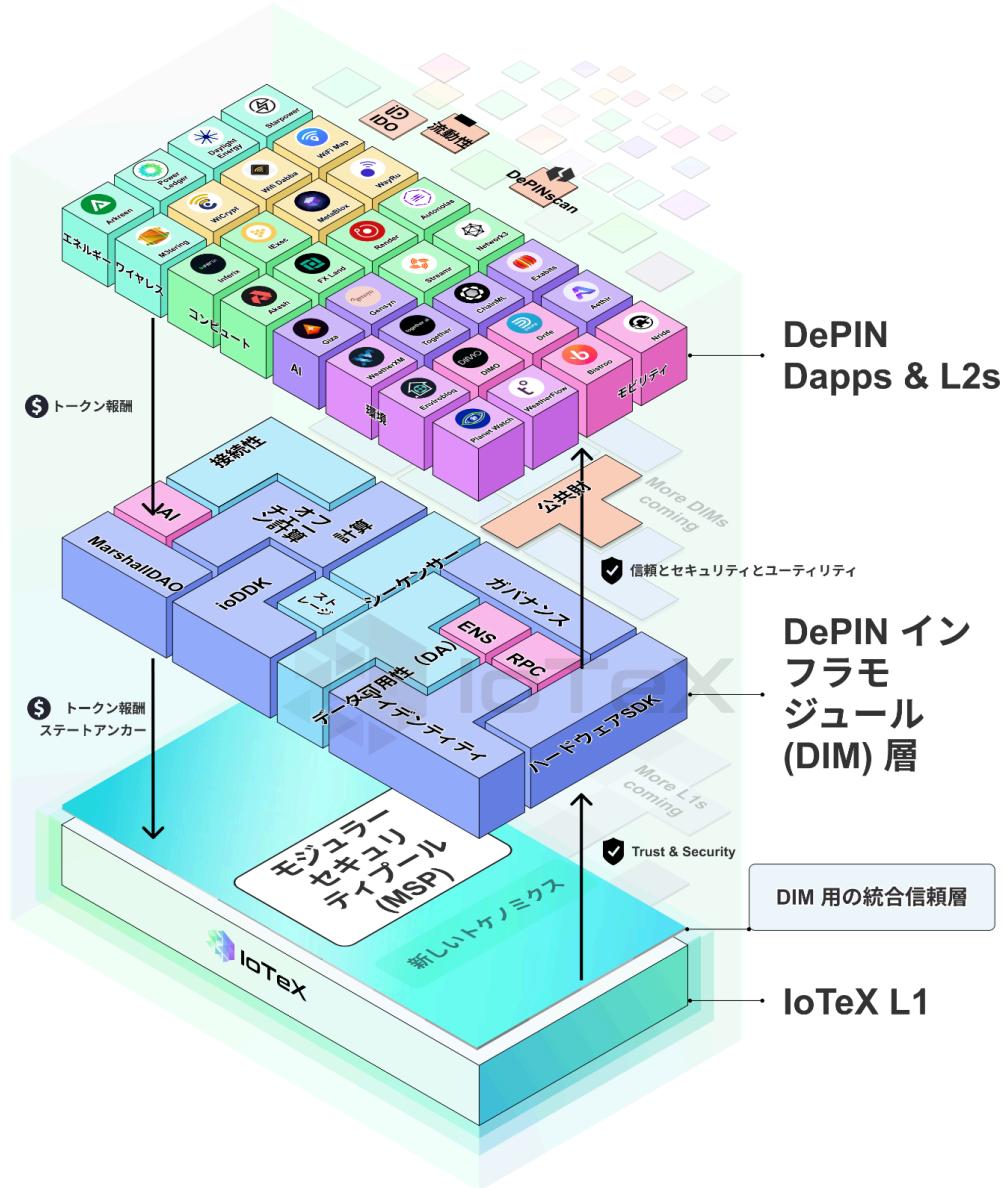


図2.1: IoTEx 2.0の範囲

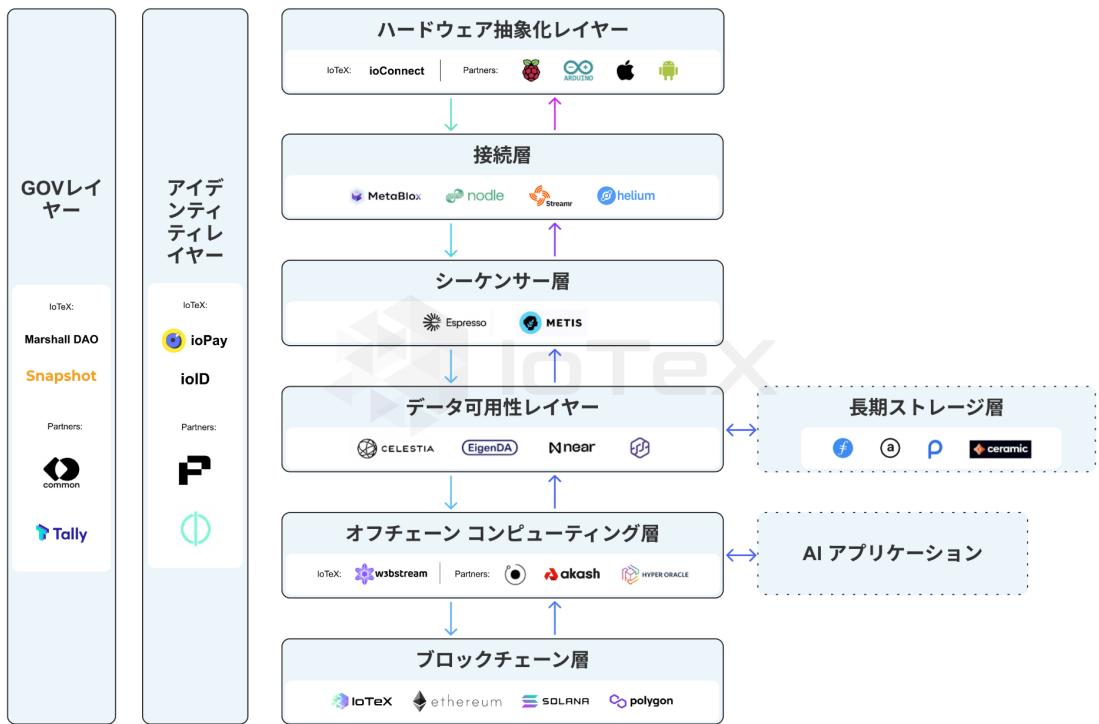


図 2.2: DePIN インフラストラクチャ モジュール (DIM)

ゼロ知識証明 (ZKP)、信頼できる実行環境 (TEE)、マルチパーティコンピューティング (MPC)、完全準同型暗号化 (FHE) などの検証可能なコンピューティングテクノロジーにより、さまざまなベンダーが「現実世界の活動の証明」をリアルタイムで生成し、これらの証明をブロックチェーンに決済してデバイス所有者に報酬を与えます。

- **ioID (Identity DIM):** 中央集権型アイデンティティプロバイダーに依存せずに、人々とマシンが豊かなデジタル関係を確立し、相互にやり取りできるようにする、オントリニティおよびオフチェーンの自己主権型デジタルアイデンティティのスイート。

- ioConnect (ハードウェア抽象化DIM):さまざまなハードウェアをW3bstreamおよびさまざまなL1/L2に接続できるようにするSDK。Raspberry Pi、ESP32、Arduinoなどの主流のハードウェアプラットフォーム上でシームレスに動作するハードウェア抽象化レイヤーで、ハードウェアを扱う複雑さ。言い換えれば、ioConnectはさまざまなDePINアプリに簡単に統合でき、マルチマイナー。
- oDDK (L2 SDK DIM): DePINビルダーがシームレスに連携できるようにするチェーンSDK。IoTeXのセキュリティを享受しながら、独自のL2ブロックチェーンを簡単に開始できます。L1。W3bstream、ioID、De-PINscanなどのIoTeXモジュールをネイティブにサポートします。
- IoTeX L1: IoTeX L1ブロックチェーンはEVMと互換性があり、社内のRoll-DPoSコンセンサスメカニズムを実行して1,000以上のTPSを実現します。IoTeX L1の利便性はIoTeX 2.0で拡張されます。ioIDはIoTeX L1に登録されたMSPは、スマートコントラクトとして展開されます。IoTeX L1とoDDKはL2チェーンをIoTeX L1に固定します。
- 私たちは、DePINScan [23] や DePIN Liquidity Hub [21] などの既存の公共財を成長させ続けるとともに、DePINビルダー向けの公共財を構築していきます。

2.3 Tokenomics

IOTXトークンは、IoTeX L1の基礎通貨として2019年に導入されました。メインネットの立ち上げ以来、IOTXトークンはバリデータ（または「デリゲート」）、Dappビルダー、ユーザーの間でインセンティブのバランスを効果的に取ってきました。IOTXをステークし、ネットワークコンセンサスの一環としてブロックチェーントランザクションを検証するデリゲートはIOTX報酬を受け取ますが、Dappsやトークン所有者などを構成する開発者とユーザーはトランザクションを送信し、スマートコントラクトと対話するためにIOTXに支払います。IOTXトークン

は、ネットワーク全体のガバナンスに参加するために、さまざまなタイプのトークン所有者によってステークされています。

IoTeX が単なる L1 から相互接続されたインフラストラクチャのモジュラー プラットフォームに拡張されると、IOTX トークンに関連するトークンノミクスも拡張されます。

IoTeX 2.0 のビジョンに適合します。これには、IoTeX の新しいテクノロジー製品に組み込まれる、IOTX トークンの新しい形式のユーティリティが含まれます。

2.0。さらに、IoTeX 2.0 トークンノミクスのもう 1 つの重要な目標は、プラットフォームの使用状況に基づいて、インフレ的なステーキング報酬とデフレ的なトークンの燃焼のバランスをとり、DePIN Dapps と L2 がモジュラー インフラストラクチャを利用するよう奨励することです。これは、アップグレードされたトークンノミクスが、W3bstream、ioID、ioDDK、その他の DIM にリンクすることで IOTX トークンに新たな有用性と価値をもたらすだけでなく、インフレとデフレのメカニズムのバランスを通じて安定したトークン供給を維持することを意味します。

IoTeX のモジュラー インフラストラクチャ製品の採用が増えるにつれ、IOTX トークンは IoTeX 2.0 ネットワークの通貨として新たな価値を生み出すことになります。

2.3.1 IoTeX 2.0 の IOTX ユーティリティ

IOTX トークンは IoTeX 2.0 インフラストラクチャとエコシステム全体で使用され、図 2.3 と 2.4 に示すように、さまざまな観点から見ることができます。

- **IoTeX L1 の観点から:** 代表者は、ネットワークトランザクションを検証してコンセンサスに参加する資格を得るために IOTX をステークし、サービスの報酬として IOTX トークンを受け取ります。トークン所有者は、代表者に投票するために IOTX をステークし、IOTX 報酬を受け取ることもできます。IOTX トークンは、IoTeX 2.0 でも IoTeX L1 ブロックチェーンのネイティブ通貨として機能し、IoTeX L1 ブロックチェー

ンでスマートコントラクトを展開してトランザクションを処理する Dapps は、ガス料金として IOTX を消費します。ガバナンスに参加するために IOTX をステークすることに加えて、ユーザーは、IoTeX L1 でトランザクションを処理するためにガス料金として IOTX を消費し、資本とリソースを提供して報酬を獲得することで Dapps とやり取りすることができます。IoTeX 2.0 では、デバイス所有者は IOTX をバーンしてデバイスを IoTeX L1 に登録し、DePIN に参加するための信頼できるアンカーとなる ioID を受け取ることもできます。最後に、ライホイールを作成するために、IoTeX L1 は DAO を採用し、トークン保有者はネットワークインセンティブの割り当て方法を投票することができます。

L1 ネイティブ トークン R

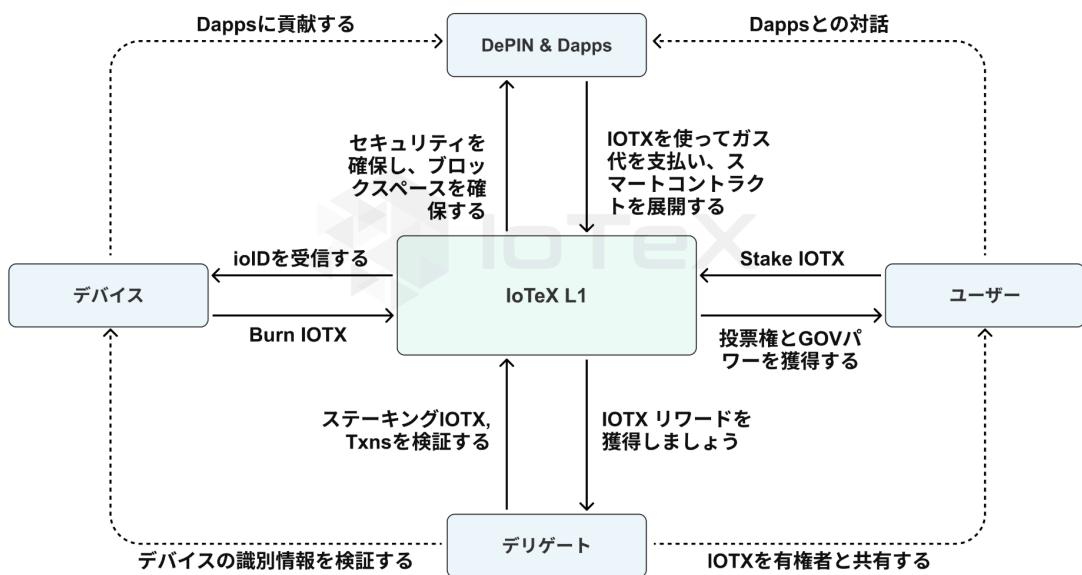


図2.3: DePINライホイールとIOTXトークンのユーティリティ

新しいデバイス、DePIN、Dapps、およびユーザーを促進することを目的としたさまざまな取り組み。より多くのデバイス、DePIN、Dapps、およびユーザーがオンボードされるほど、IOTX のバーン、ステーキング、および使用を通じて、IoTeX L1 での IOTX のユーティリティが高まります。

- モジュラー セキュリティプール (**MSP**) の観点から: IoTeX 2.0 では、ユーザーは、モジュラー セキュリティプール (MSP) に再ステーキングまたは再担保することで、ステーキングした IOTX を再利用できるようになります。モジュラー セキュリティプールは、IoTeX 2.0 にサービスを統合する DIM に IoTeX L1 ブロックチェーンのセキュリティを拡張するように設計されています。MSP を使用すると、DIM ビルダーは、IOTX ステーカーに再ステークされた IOTX を割り当ててソリューションのセキュリティを提供するようインセンティブを与えることができます。これにより、IOTX をステークする必要がある DIM に MSP がセキュリティと信頼を事実上「リース」する、ステークされた IOTX を組み込んだ新しい経済が導入されます。新しいデバイス、DePIN、Dapps、およびユーザーを促進することを目的としたさまざまな取り組み。より多くのデバイス、DePIN、Dapps、およびユーザーがオンボードされるほど、IOTX のバーン、ステーキング、および使用を通じて、IoTeX L1 での IOTX のユーティリティが高まります。図2.3: DePINフライホイールとIOTXトーケンのユーティリティこれにより、IOTXステーカーにとって新たな収益機会が生まれ、同じ基本IOTXステーキング報酬に加えて追加の報酬も獲得できるようになります。

MSP & DIMs

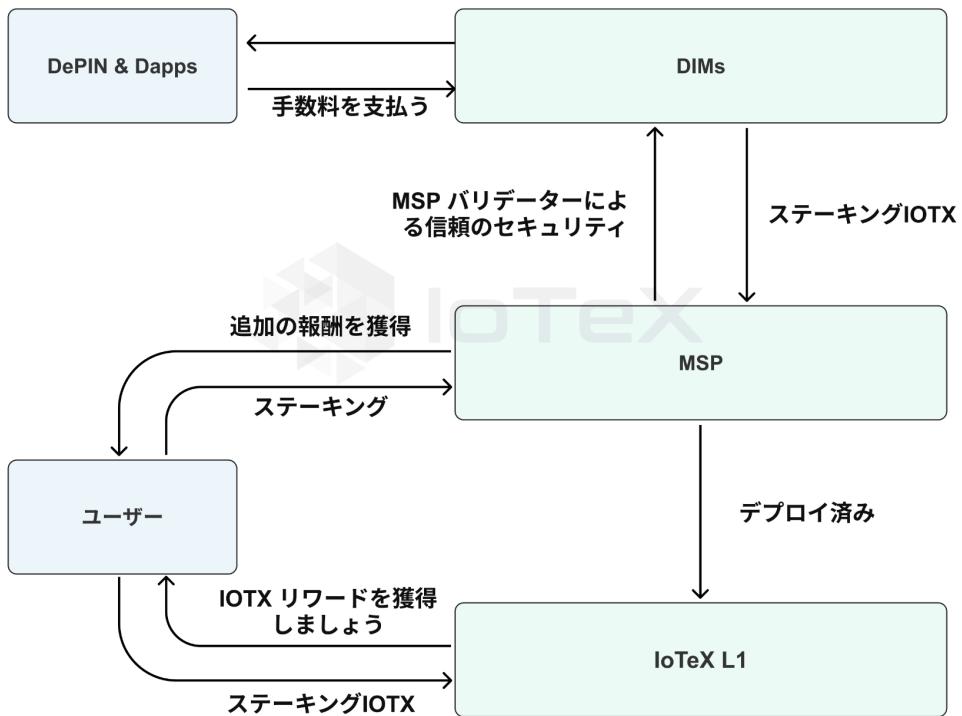


図2.4: MSPとDIMにおけるIOTXトークンの有用性

ステークしたIOTXトークンの再ステーク、およびDIMプロジェクトからの賄賂の可能性。

- **DePINインフラストラクチャモジュール(DIM)**の観点から: DIMは、モジュラーセキュリティプール(MSP)に参加し、再ステークされた資産のプールからセキュリティを獲得し、検証可能な方法でDapps、L2、およびユーザーにサービスを提供するため、IOTXをステークする必要があります。DIMは、サービスを活用するDappsからの支払いとしてIOTXを使用することも、独自のトークンを使用することもできます。たとえば、Filecoinなどの長期ストレージプロバイダーやNEARなどのデータ可用性プロ

バイダーは、IOTXをステークしてIoTeX 2.0にDIMとして参加し、その後、独自のトーケンでデータサービスに対してDappsに課金できます。

- **DePIN Dapps と DePIN L2s の観点から:** IoTeX 2.0 テクノロジー スタックで起動する Dapps と L2s は、トランザクションを処理し、スマートコントラクトとやり取りするために IOTX を支払います。さらに、Dapps と L2 チェーンは独自のモジュール式テクノロジー スタックを選択し、接続、データストレージ、オフチェーンコンピューティングなどのサービスに対して 1 つ以上の DIM に DIM のトーケンで支払うことができます。ループを閉じるために、ほとんどの Dapps には、ユーザーが取得して Dapps サービスにアクセスするために使用する独自のトーケンがあります。

上記の IOTX トーケンのユーティリティに加えて、図 2.5 に示すように、インフラストラクチャの使用状況に基づいて IOTX トーケンがバーンされる方法、インセンティブプログラムを介して IOTX が Dapps やビルダーと共有される方法、今後新しい IOTX がステーカーに発行される方法に関する IoTeX 2.0 の新しい設計もあります。次のサブセクションでは、これらの新しい設計について説明します。

IOTXの発行、デフレーション、および再ステーキング

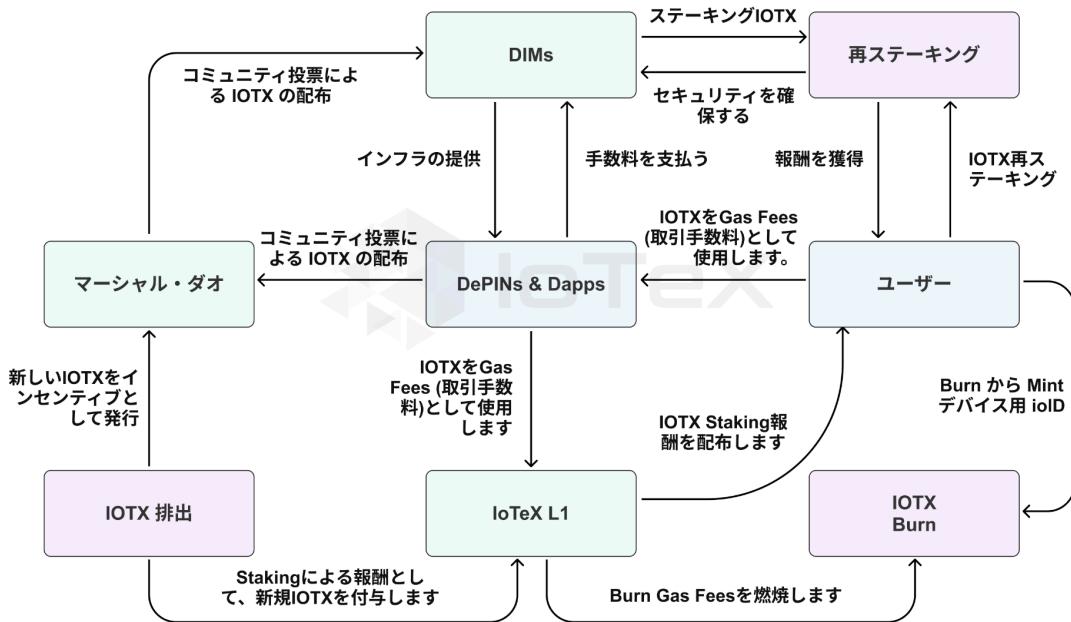


図2.5: IoTeX 2.0におけるIOTXトークンの発行、デフレーション、再ステーキング

2.3.2 インフレステーキング報酬

IoTeX メインネットが 2019 年に開始されたとき、IOTX の総供給量の 12% (つまり、12 億 IOTX) がデリゲートのステーキング報酬に割り当てられました。トークン保有者は IOTX をステーキングしてデリゲートに投票し、デリゲートはステーキング報酬の一部を投票者と共有します。2019 年以降、ブロック報酬とエポック報酬の形で、年間約 2 億 IOTX がデリゲートと投票者に分配されています。ブロック報酬は、新しいブロックが生成されるたびにコンセンサスデリゲート (つまり、ブロックを生成する資格のある上位 36 人のデリゲート) に配信され、エポック報酬はエポックごとに (つまり、1 時間ごとに) 上位 100 人のデリゲートに比例配分されました。メインネットが稼働してから 4 年以上が経過し、ステーキング報酬用に当初割り当てられた IOTX 供給量はほぼ完全に分配されつつあります。そのため、IoTeX 2.0

の一部としてインフレステーキング報酬が導入され、デリゲートがネットワークトランザクションの検証とネットワークの保護を継続するよう奨励されます。

インフレステーキング報酬は、トークン供給に追加された新しい IOTX として定義され、コンセンサスに参加するデリゲートと IOTX をステーキングするトークン保有者に配信されます。基本的に、これは IOTX トークンをステーキングした人だけが新しく発行された IOTX トークンを受け取ることを意味し、これにより IOTX のステーキング比率が高まり、IoTeX ネットワーク全体のセキュリティが向上します。インフレステーキング報酬の分配は、ステーキング報酬に割り当てられた以前の IOTX 分配と同じ構造に従います。ブロックを生成するコンセンサスデリゲートはブロック報酬を獲得し、上位 100 人のデリゲートはエポック報酬を比例配分します。

これはIoTeXネットワークにとって新しい概念ですが、インフレステーキング報酬は、イーサリアム、ソラナ、コスマスなど、ほぼすべてのL1に組み込まれています。たとえば、ソラナは8%のインフレ率で始まり、毎年15%減少しています。2024年第1四半期の時点で、ソラナネットワークのインフレ率は約5.5%です。IoTeXネットワークの実際の年間インフレ率はネットワーク全体のガバナンスによって決定されますが、目標は、他のブロックチェーンエコシステムと比較してIoTeX L1デリゲートに競争力のあるステーキング報酬APRを提供する稳やかなインフレを導入し、DIMとDePINアプリが成長を維持しながらインセンティブを与えることです。トークンのデフレバーンを考慮した場合の安定したトークン供給。詳細は以下のセクションをご覧ください。

2.3.3 デフレ燃焼

暗号ネットワークで必要なインフレのバランスをとるために、ネットワークの使用状況に基づいたトークンのデフレバーンが一般的に実装され、安定したトークン供給が維持されます

(例: Burn and Mint Equilibrium はそのような設計パターンです)。たとえば、Ethereum ネットワークはバリデーターに 1 日あたり約 1,700 の新しい ETH を発行しますが、このインフレとガス料金のデフレバーン (つまり、EIP-1559) のバランスをとることで、時間の経過とともに全体的に安定した、またはデフレの ETH トーカン供給を維持します。2020 年以降、IoTeX ネットワークは、ネットワークに登録された新しいデバイスの数に基づいて IOTX のデフレバーンを促進するために Burn-Drop プログラムを利用しておらず、その結果、これまでに総供給量の約 4% または 400M IOTX がバーンされています。IoTeX 2.0 の導入と Burn-Drop プログラムの終了により、モジュラー インフラストラクチャの使用状況に基づいて、プロトコルレベルで IoTeX ネットワークに新しいデフレバーンソースが追加されます。

- L1 レベルでは、IoTeX 2.0 は Ethereum の EIP-1559 に似たガス料金のバーンを導入します。これにより、IOTX へのインセンティブが与えられ、価値が再分配されます。トーカンのデフレバーンを考慮した場合の安定したトーカン供給。詳細は以下のセクションをご覧ください。IoTeX L1 の使用増加に基づくトーカン保有者。ガバナンスに参加し、代表者に投票するための IOTX のステーキングは変更されず、ステーキングされた資産が IOTX トーカンの速度を低下させる重要な効果を維持します。
- ioID の場合、デバイスの新しいオンチェーン ID の作成には、一定量の IOTX を書き込む必要があります。書き込み速度は、IoTeX ネットワークに登録されているデバイスの総数に基づいて動的に変化します。さらに、ioID の設計には、DID の検証可能な資格情報 (VC) を取得するための追加のデフレ燃焼メカニズムが組み込まれます。たとえて言えば、ioID は空のパスポートに似ており、VC は人々がさまざまな国にアクセスできるようにするパスポートのスタンプに似ています。IoTeX 2.0 では、ioID が IoTeX L1 に登録され、IOTX トーカンをバーンして W3bstream などの DIM にアクセスすることで、デバイスの 1 つ以上の VC が取得されます。この設計では、IoTeX ネットワーク内の「装備」されたデバイスの数の増加に基づいて、IOTX トーカン保有

者に価値が再分配されます。Burn-Drop に似ていますが、IoTeX 2.0 のモジュール設計とよりよく一致するように再設計されています。

- W3bstream、ioConnect、ioDDK の場合、Dapps や企業によるこれらのモジュール製品の成長と採用によって促進されるネットワーク効果により、デバイスがそれぞれの DIM と直接対話する必要があるため、IOTX のデフレバーンが促進されます。さらに、IoTeX コミュニティによって定義された採用しきい値に基づいて IOTX トークンを定期的にバーンし、トークン所有者に価値を再分配することもできます。

IoTeX 2.0 トークノミクスは、IOTX トークンのデフレバーンを促進することで、IoTeX プラットフォームのさまざまなモジュールコンポーネントの使用増加に報いるように設計されています。当初、このデフレバーンは、上記のインフレステーキング報酬を相殺して、安定した総トークン供給を維持し、将来的には IoTeX プラットフォームの大量導入により、IOTX トークンの総供給が純デフレになる可能性があります。これを達成するために必要な大量導入を促進するために、IoTeX 2.0 トークノミクスは、以下に説明する成長インセンティブプログラムを通じて、さまざまなビルダーに IOTX トークンを割り当てます。

2.3.4 成長インセンティブ

IoTeX 2.0 の重要な柱は、Marshall DAO (IIP-23) [10] です。これは、IoTeX の利害関係者が、評判の良い DePIN プロジェクトの参加やネットワーク全体のイニシアチブへの資金提供など、IoTeX エコシステムを成長させるために IOTX インセンティブをどのように配分するかについて提案できるようにする、分散型自律組織 (DAO) です。これにより、最高のアイデアが IOTX を使用して資金提供される、透明で実力主義のシステムが生まれます。Marshall DAO は、当初、BurnDrop 割り当てから再利用された 5 億 IOTX 以上によって資金提供されます。これは、2024 年第 1 四半期に IoTeX コミュニティによるネットワーク全体の投票によって

決定されました。将来的には、マーシャルDAOへの追加資金がさらに追加される可能性がある。新しく発行された IOTX をプールに追加するためのネットワーク全体の投票。

図 2.6 に示すように、Marshall DAO は投票エスクロー オンチェーン ガバナンス モデルを採用しています。これは、DAO に賭けられる IOTX が増えるほど、ユーザーが持つ投票権が増えることを意味します。これにより、プロジェクトやイニシアチブへの資金提供の決定は、IoTeX の長期的な成功に最も注力している人々によって行われることが保証されます。少なくとも 91 日間ステークするトークン所有者は、譲渡不可能なオンチェーントークンである veIOTX を獲得します。これは、特定の提案を表すゲージを介して資金割り当ての提案と投票に使用できます。これは、長期投資家が veIOTX を使用して投票して、IoTeX 上の DEX 取引ペアの流動性の向上、ローンチパッドを介した初期段階の DePIN プロジェクトのスポンサー、DePIN の加速などを含むがこれらに限定されないさまざまなプロジェクトに DAO からの IOTX が資金を供給する方法を決定できることを意味します。デュアルマイニングによる PIN プロジェクト、公共財やネットワーク全体のツールに対する助成金の発行など。

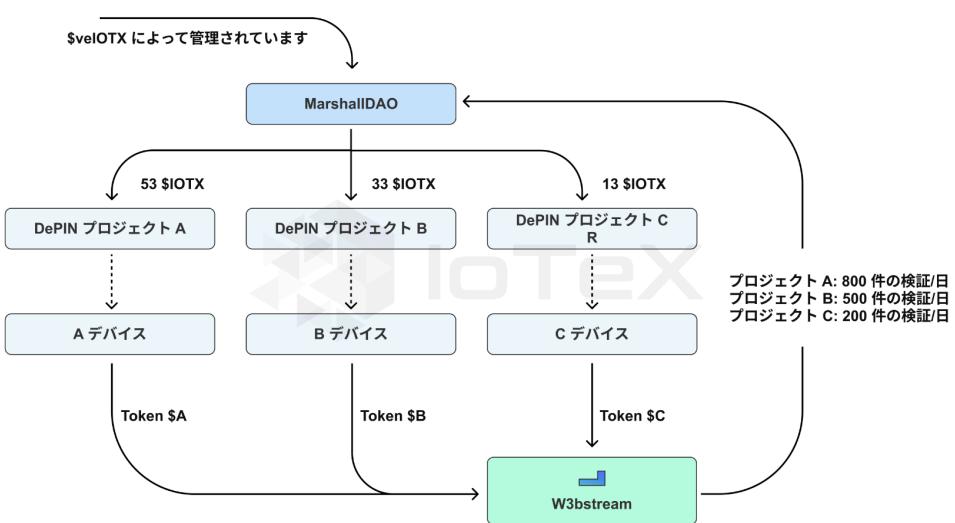


図2.6: マーシャルDAOガバナンスモデル

2.4 公共財

IoTeX ブロックチェーンと DIM によって提供される機能に加えて、De-PIN プロジェクトの短期的 および中期的な課題の多くに対処する公共財も IoTeX 2.0 の重要な部分です。これらの公共財は、シンプルな統合を通じて DePIN プロジェクトに認知度、使いやすさ、流動性を提供するとともに、IoTeX コミュニティに、より広範な DePIN 業界を監視し、特定のプロジェクトを深く掘り下げる方法を提供します。

- DePINScan [23] は、DePIN セクターの業界全体の探索者です (図 2.7 を参照)。これは、DePIN のユーザー、マイナー、投資家が DePIN プロジェクトの成長を監視し、初期段階のプロジェクトを発見できるように設計されています。リアルタイムのデバイス数とプロジェクトプロファイルを提供し、プロジェクトを発見し、DePIN 資産の価格、量、時価総額をリアルタイムで取得する方法として機能します。

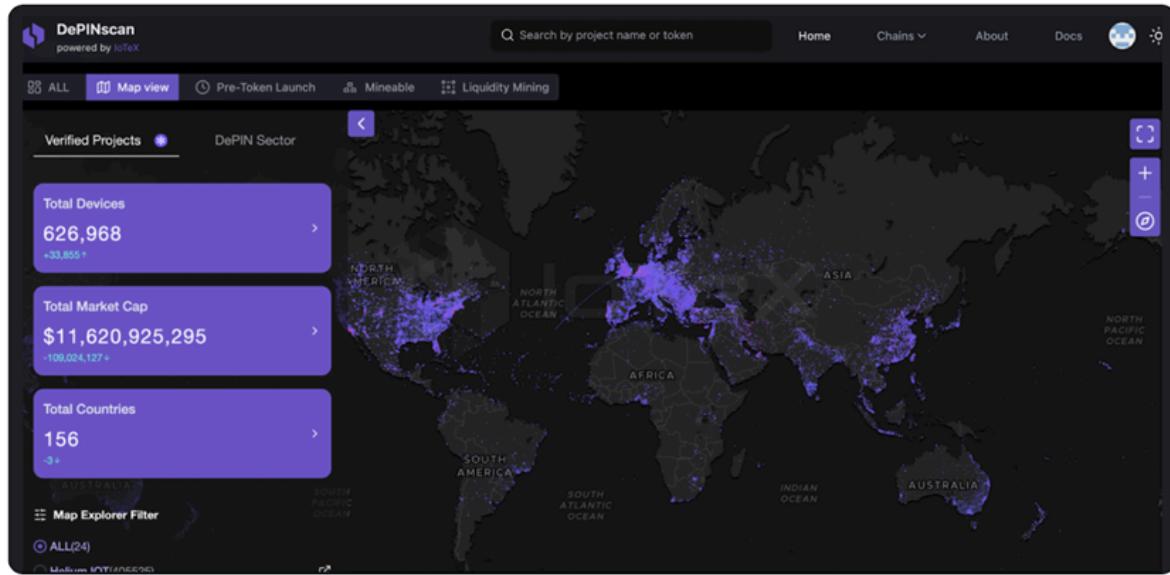
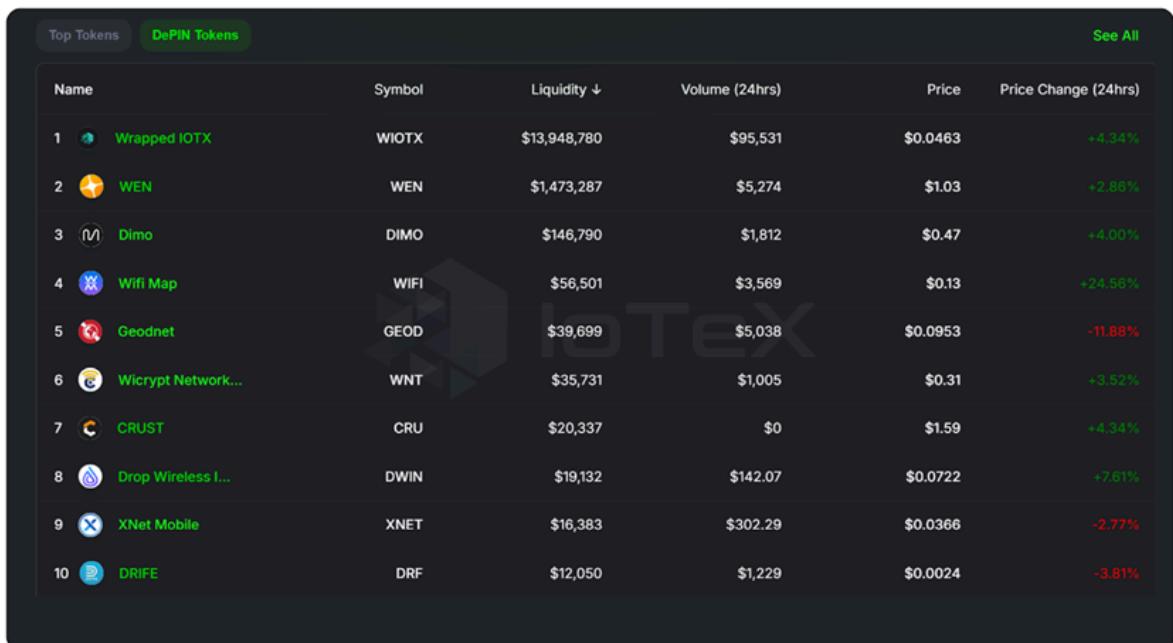


図 2.7: DePINScan エクスプローラー

- DePIN Liquidity Hub [21] は、自動化されたレンジマネージャー（マーケットメーカー）と、ユーザーは DePIN トークンを取引できるようになります（図 2.8 を参照）。
 トークンの流動性は、あらゆる暗号プロジェクト、特に DePIN にとって、ネットワークを成長させるためのインセンティブ メカニズムとしてトークンを多用するため、非常に重要です。残念ながら、初期段階の DePIN の多くは、健全なレベルのオンチェーン流動性を構築し維持することに苦労しています。新しいプロジェクトをサポートするために、IoTeX は DePIN 流動性ハブ [24] を立ち上げ、他の L1 チェーンから IoTeX L1 にトークンをブリッジし、さまざまな分散型取引所（DEX）上に両面流動性プールを作成できる DePIN プロジェクトの流動性を高めます。そして、投資家にオンチェーン流動性をブーストアップするよう奨励する流動性マイニングキャンペーンを実施します。



The screenshot shows a dark-themed web application interface for the IoTeX DePIN Liquidity Hub. At the top, there are two tabs: "Top Tokens" (highlighted in blue) and "DePIN Tokens". On the right side of the header, there is a "See All" link. The main content area displays a table with 10 rows, each representing a DePIN token. The columns are: Name, Symbol, Liquidity ↓, Volume (24hrs), Price, and Price Change (24hrs). The tokens listed are: 1. Wrapped IOTX (WIOTX), 2. WEN (WEN), 3. Dimo (DIMO), 4. Wifi Map (WIFI), 5. Geodnet (GEOD), 6. Wicrypt Network... (WNT), 7. CRUST (CRU), 8. Drop Wireless I... (DWIN), 9. XNet Mobile (XNET), and 10. DRIFE (DRF). The table includes a large watermark for "IoTeX" in the center.

Name	Symbol	Liquidity ↓	Volume (24hrs)	Price	Price Change (24hrs)
1 Wrapped IOTX	WIOTX	\$13,948,780	\$95,531	\$0.0463	+4.34%
2 WEN	WEN	\$1,473,287	\$5,274	\$1.03	+2.86%
3 Dimo	DIMO	\$146,790	\$1,812	\$0.47	+4.00%
4 Wifi Map	WIFI	\$56,501	\$3,569	\$0.13	+24.56%
5 Geodnet	GEOD	\$39,699	\$5,038	\$0.0953	-11.88%
6 Wicrypt Network...	WNT	\$35,731	\$1,005	\$0.31	+3.52%
7 CRUST	CRU	\$20,337	\$0	\$1.59	+4.34%
8 Drop Wireless I...	DWIN	\$19,132	\$142.07	\$0.0722	+7.01%
9 XNet Mobile	XNET	\$16,383	\$302.29	\$0.0366	-2.77%
10 DRIFE	DRF	\$12,050	\$1,229	\$0.0024	-3.81%

図2.8: DePIN流動性ハブ

ビルダーがすでに利用できる上記の公共財に加えて、IoTeX 2.0 の開発全体を通じて IoTeX チームや世界的なビルダーによって構築される公共財もあります。例としては、DePIN プロジェクトを熱心な投資家に提供するための DePIN プロジェクトの出発点、DePIN に焦点を当てたハードウェアをマイナーに公開するためのデバイスマーケットプレイス、および DePIN プロジェクトの分散投票。IoTeX 2.0 は、建設業者が公共財を容易に利用できるようにすることで、DePIN プロジェクトの立ち上げと成長をこれまで以上に容易にする一連の機能をプロジェクトに提供します。

2.5 プロジェクトライフサイクル全体を通じてビルダーをサポートする

IoTeX 2.0 は、実力主義のトークノミクスによって管理される、幅広いインフラストラクチャ、ツール、およびパブリックリソースを提供します。これらは、図 2.9 に示すように、プロジェクトライフサイクルのあらゆる段階で DePIN ビルダーを支援するように設計されています。



図 2.9: DePIN プロジェクトライフサイクル全体にわたるサポートビルダー

- 初期段階では、DePIN プロジェクトは主に技術スタックの開発とプロジェクトの認知度の向上に重点を置いています。これを促進するために、IoTeX 2.0 は DePINscan や Liquidity Hub などのパブリックリソースを提供して、注目を集め、流動性を高め、ユーザーを獲得します。
- プロジェクトが進むにつれて、特にプロジェクトが技術スタックを分散化し、より高いスクエーラビリティを目指すにつれて、より高度で適応性の高いインフラストラクチャの需要が高まります。これらのニーズに応えるために、IoTeX 2.0 は、W3bstream、ioID、ioConnect などのインフラストラクチャを提供し、DePIN ビルダーに最先端のテクノロジーを提供します。
- 長期的には、DePIN プロジェクトは独自の需要と供給のネットワークを確立し、拡張する必要があります。IoTeX 2.0 は、ioDDK を介して独自の L2 を起動できるようにすることで、後期段階でもこれらのプロジェクトをサポートし続けます。

2.6 将来

IoTeX 2.0 により、私たちは世界中のデバイスに自己主権を実現するために必要なすべてのツールを装備し、現実世界のインテリジェンスをコンパイルして革新的な Dapps を強化し、ユーザーが独自のサービスとインテリジェンスを自分のデバイスから収益化できるようにするという新たな旅に乗り出しています。デバイス。現在進行中の人工知能、ブロックチェーン、スマートデバイスの融合は、世界の仕組みを根本的に変える技術革命を引き起こしています。これらのテクノロジーは時間の経過とともに個別に進化してきましたが、ますます絡み合い、新しい生産的な資産、つまり信頼できるユーザー所有のデバイスで構成される DePIN ネットワークにパッケージ化されるようになってきています。

スマートデバイスはサービスを提供し、データを生成します。ブロックチェーンは、これらのデータとサービスに信頼性と検証可能性を追加します。そして最後に、AI がデータから価値を抽出し、これらのサービスを自動化します。ほんの数年前までは SF のように思えたことが、今では現実になりつつあります。近い将来、新興機械経済はこのテクノロジー三位一体によって推進され、世界で最も価値のある産業になるでしょう。ブロックチェーンを使用すると、社会に利益をもたらすだけでなく、日常の人々に価値と公平性を提供する信頼できるテクノロジーを使用して、この新しいマシン経済をプログラムできるようになります。可能性は無限ですが、最もエキサイティングな機会には次のようなものがあります。

- **集合的インテリジェンスと AI: IoTeX** は、リアルタイム情報を集約するための最大のデバイスハブ、つまり現実世界のデータハブになります。デバイスからデータストリームをキャプチャし、現実世界のイベントをオンチェーンで検証することで、大衆の集合知をクラウドソーシングして、接続、スマートシティ、再生可能エネルギーなどの個別の業界に革命を起こすことができます。AI を利用して業界間の関係を分析し、世界に対する私たちの理解を進化させる関係性の洞察を抽出することには、さらに大きなチャンスが潜んでいます。IoTeX 2.0 は、スマートデバイスの目を通して現実世界の歴史を記録する分散型プラットフォームとなり、過去を理解して未来を最適化でくるようになります。
- **自律型マシンエコノミー:** スマートデバイスは、貴重なデータを生成するだけでなく、信頼できる価値のあるサービスを人々に提供するために進化しています。自動運転タクシーは初の無人乗車を実現し、衛星は世界中の人々に接続を提供し、倉庫では人間の器用さを超えたロボットを利用し、太陽光エネルギーと風力エネルギーは次世代の再生可能エネルギー装置によって生産されています。これらのサービス提供デバイスのオーケストレーションは、ブロックチェーンとインテリジェント AI を使用して最適に実行されます。私たちは、IoTeX によって AI システムが前例のない精度と

完全な信頼性で地球資源を監視および管理できるようになる未来を思い描いています。

- デジタルリソースマーケットプレイス: 一部の DePIN は場所に依存するハードウェアからのデータとサービスに焦点を当てていますが、他の DePIN は場所に依存しないハードウェアからデジタルリソースを集約します。これらには、デジタルストレージ、CPU および GPU を介したコンピューティング、帯域幅、およびクラウド複合企業によって従来提供してきたその他のデジタルリソースが含まれる場合があります。「データは新たな金」、「コンピューティングは新たな石油」の時代に、IoTeX 2.0 により、貴重なデジタルリソースをクラウドソーシングしてマーケットプレイスに投入し、誰もが世界中の他のユーザーとピアツーピア方式でリソースを交換できるようになります。
- 分散型ガバナンスと意思決定: 現実世界のデータを安全かつ透過的にブロックチェーンに統合することにより、IoTeX 2.0 は、現実世界の出来事に関する検証可能な事実を使用した分散型意思決定の基盤を確立するのに役立ちます。人間が分散ガバナンスを通じて集合的にプロセスを定義することで、不変のスマートコントラクトと安全なデバイスを利用して、社会の主要な側面を信頼できる方法で運用できます。IoTeX 2.0 は、誰でも自分の専門知識を提供し、新しい世界のオープンガバナンスに参加できる手段を提供します。

第3章

モジュラー セキュリティプール (MSP) -

DePIN インフラストラクチャ モジュール用の

統合信頼層

3.1 問題

DePIN は、シナリオ固有の DePIN L2 などのオンチェーン要素と、データストリーム、オラクル、プロセス、検証、ストレージ、自動化などのオフチェーン要素の両方を含む包括的な技術スタックを備えています。この複雑な構造では、独自の分散型信頼アーキテクチャをゼロから作成するために、より多くのモジュールとビルダーが必要になります。タスクには、ステーキングトークンの設計、流動性の創出、ステーカーの誘致、バリデーターの採用、市場での採用が含まれる場合があり、セキュリティと分散化の潜在的な断片化につながります。

分散化された方法で統一されたエンドツーエンドの信頼を確立するには、最も弱いリンクの原則に従って、各部分が可能な限り安全かつ分散化されていることを確認することが重要です。開発者が DePIN インフラストラクチャ モジュール (DIM) の開発を続ける中で、断片化のないセキュリティと分散化の整合性を維持することが優先事項となっています。このアプローチにより、DePIN プロジェクトで使用するために、既存の技術スタックに DIM を迅速に統合できます。モジュラー セキュリティプール (MSP) は、DIM をサポートする統合信頼レイ

ヤーを提供します。これは、確立されたさまざま な L1/L2 からステーキング セキュリティを収集し、報酬と引き換えにそのセキュリティを新しい DIM に貸し出すことができます。このシステムにより、新しいインフラストラクチャ モジュールは、独自のセキュリティインフラストラクチャを構築することなく、基盤となる L1/L2 のセキュリティの恩恵を受けることができます。たとえば、新しい DIM はガバナンス提案を通じて MSP に参加できます。承認されると、DIM は L1/L2 のセキュリティと分散化を採用し、IoTeX エコシステム プロジェクトからプロトコルの使用を許可されます。特定の DIM をサポートするステーカーは、ステークを MSP に向けることで、DIM ネットワークトー クンの形で報酬を受け取ることができます

3.2 安全と信頼のためのオープンマーケット

MSP は、ステーカーと DIM によるプールされたセキュリティの供給と消費を巧みに管理するオープンな市場メカニズムを自信を持って提示します。MSP は、多数の DIM 間でセキュリティを分散させるのではなく、すべての DIM にわたって DePIN に重点を置いたセキュリティを統合します。具体的には、MSP には 3 種類の参加者がいます。

- **DIM ビルダー**は、シナリオ固有の DePIN L2、データストリーミング、オラクル、処理（汎用、ZKP ベース、TEE ベースなど）、データストレージ、自動化（自動支払い、価格フィードなど）、ID、認証モジュールなどの DIM を構築します。DIM ビルダーは、ステーカーにインセンティブを与えて、資産をモジュールに割り当てるようになります。MSP は、ステーカーが DIM から十分にインセンティブを得られるよう、賄賂のメカニズムを提供します。
- **ステーカー**は、十分に確立されたブロックチェーンから 1 つ以上のバリデーターに資産を委任するネットワーク参加者です。ノード自体を実行する必要がなく、ネットワークセキュリティに貢献します。彼らは、代表団への見返りに、ネットワークの手数料と報酬の一部を受け取ります。戦略的な割り当てにより、さらなるスラッシュの可能

性を考慮して、追加のプールされたセキュリティに値するモジュールが決定されます。ステーカーは、MSPが自分たちの資産に追加の大幅な条件を課すことを許可することでオプトインし、経済的安全性を強化します。ここで、私たちが構築している MSP インフラストラクチャはオープンソースであり、短期的には IoTeX L1 のセキュリティを利用できるようになり、将来的にはビットコイン、イーサリアム、Solana を含むすべての主要なブロックチェーンのセキュリティを利用できるようになることに注意することが重要です。

- バリデーターは、DePIN プロジェクトに直接サービスを提供する DIM ビルダーが利用できる、常時実行されているノードのセットを提供します。

MSP の実装には、次の主要原則が組み込まれる必要があります

- オープンな参入と退出:ステーカーと DIM は、制限なく市場に参入および退出する自由を持つ必要があります。これにより、サービスの真の価値を反映した競争力のある価格設定が保証されます。
- ネットワーク効果:参加者の数が増えると、各参加者は市場の価値をより高く評価します。この正のフィードバックループにより、より多くの買い手と売り手が市場に引き寄せられます。
- 無許可: 市場は中央当局によって管理されていません。代わりに、需要と供給の法則に基づいて動作します。

3.3 アーキテクチャ

図 3.1 に示すように、モジュラー セキュリティプール (MSP) のアーキテクチャは、確立された L1 ブロックチェーン上の既存のステーキングシステムから継承されたセキュリティに基づいて、新しいネットワーク、特に DePIN と DIM を構築するための合理的で安全なプロセスを提供するように設計されています。MSP の動作の詳細な内訳は次のとおりです。

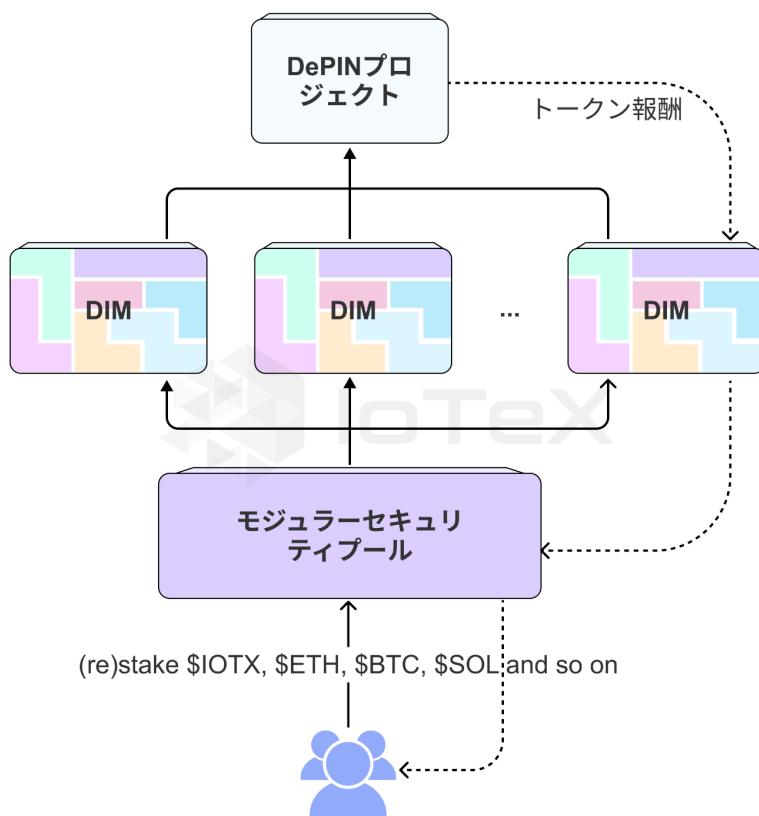


図 3.1: モジュラー セキュリティプール (MSP) のアーキテクチャ

1. .ステーカーが資産を委任:ビットコイン、イーサリアム、IoTeXなどの確立された L1 の参加者であるステーカーは、資産を MSP に委任します。これにより、ステーカーは MSP ベースのネットワークのセキュリティに貢献します。
2. ステーカーがバリデーターを選択: MSP ネットワーク内では、ステーカーは、関連付けられている DIM ネットワークによって提供されるオプションのプールからバリデーターを柔軟に選択できます。バリデーターは、ネットワークを保護し、トランザクションを検証するためにノードを実行する責任があります。
3. バリデーターがノードを運用:ステーカーによって選択されると、バリデーターは MSP ネットワーク内でノードを運用します。これらのノードは、ネットワーク全体のトランザクションの整合性とセキュリティを確保する上で重要な役割を果たします。
4. **DIM** ビルダーがネットワークを確立する:一方、DIM ビルダーはそれぞれのネットワークの開発に取り組んでいます。
5. .ステーカーへのインセンティブ: DIM ビルダーは、ステークに対し、MSP ネットワーク内のモジュールに資産を割り当てるよう奨励します。このインセンティブは、報酬、ネットワクトークン、その他の特典など、さまざまな形をとることができます。MSP は、参加を促進するための賄賂メカニズムなどのメカニズムを通じて、ステーカーが十分な動機を持っていることを保証します。
6. .ステーキング セキュリティの配布: MSP は、新しい DIM にステーキング セキュリティを配布する上で重要な役割を果たします。確立された L1/L2 から収集されたペーパルされたセキュリティと、ステーカーとバリデーターの参加を活用することで、MSP はこれらの新しいネットワークのセキュリティと分散化に貢献します。

全体として、このアーキテクチャは、新しいDIMを起動するためのより効率的で安全なプロセスを促進します。既存のL1/L2のセキュリティを活用し、ステーカー、バリデーター、ビルダーなどのさまざまな関係者を統合することで、MSPは分散型信頼アーキテクチャの革新と成長につながる堅牢なエコシステムを育みます。このアプローチは、新しいネットワーク開発者の時間とリソースを節約するだけでなく、DePINエコシステムの全体的なセキュリティと回復力を強化します。

第4章

W3bstream - DePIN 検証のための分散型 マルチ証明者ネットワーク

DePIN アプリケーションには通常、DePIN デバイスによって現実世界から収集されたデータに基づいて洞察を抽出できる専用のデータ処理シナリオ (スコアの計算、デバイスの位置特定、不正なデバイスの検出など) が含まれています。その後、その洞察は、トークン関連アクションのスマートコントラクトをトリガーするために使用されます。マシンデータは大量にあるため、それをオンチェーンで処理して保存するのは法外で非効率的です。その結果、オフチェーンコンピューティングは、DePIN のスケーラビリティの課題に対処する有望なソリューションとして浮上しました。

4.1 W3bstream アーキテクチャ

W3bstream は、IoTeX によって開発された、ブロックチェーンで調整されたマルチ証明者ネットワークであり、世界規模の異種証明者の力を活用して、新興の DePIN アプリケーションを強化することを目的としています。一言で言えば、W3bstream は、異種ノードで構成される分散型オフチェーンコンピューティング ネットワークです。W3bstream は、IoTeX によって開発された、ブロックチェーンで調整されたマルチ証明者ネットワークであり、世界規模の異種証明者の力をを利用して、新しい DePIN アプリケーションを強化します。一言で言

えば、W3bstream は、異種ノードで構成される分散型オフチェーンコンピューティング ネットワークです。

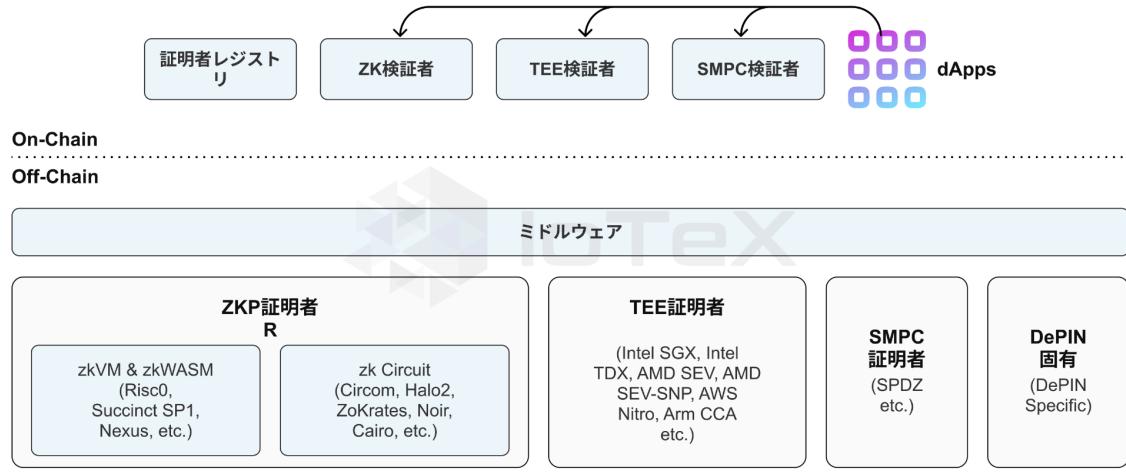


図 4.1: W3bstream の概要

4.1.1 4種類の証明者

これまで、データ処理の整合性を証明し、公開検証を可能にするために、ゼロ知識証明 (ZKP)、信頼できる実行環境 (TEE)、セキュアマルチパーティコンピューティング (SMPC) など、さまざまな技術が開発されてきました。これらの技術は、さまざまなセキュリティの前提に依存しており、実際にはさまざまな影響があります。W3bstream は、適切に設計されたミドルウェアレイヤーを通して、ゼロ知識証明 (ZKP) 証明者、信頼できる実行環境 (TEE) 証明者、セキュアマルチパーティコンピューティング (SMPC) 証明者、および Bring Your Own Prover (BYOP) という 4 つのカテゴリの証明者に対応し、DePIN アプリケーション用の検証可能な計算を実現します。

- **ZKP Prover:** ZKP は、一方の当事者 (つまり、証明者) が、特定のステートメントが真実であることを開示することなく、別の当事者 (つまり、検証者) に証明することを許可します。
- **ZKP Prover:** ZKP は、一方の当事者 (つまり、証明者) に許可します。あるステートメントが真実であるという事実以外の追加情報を開示することなく、そのステートメントが真実であることを他の当事者 (つまり、検証者) に証明すること。ZKP は、完全性、健全性、ゼロ知識の形式的要件を満たす必要があり、それによってトラストレスアプリケーションの構築が可能になります。実際には、ZKP 証明器は、汎用のゼロ知識仮想マシン (zkVM) またはカスタマイズされた制約システム (つまり、回路) を使用して実現できます。zkVM (カスタマイズされた回路) 上に構築された SNARK ベースのアプリケーションの典型的なシステムアーキテクチャを図 4.2 および 4.3 に示します。



図 4.2: zkVM 上に構築された SNARK ベースのアプリケーションのシステムアーキテクチャ

汎用の zkVM ベースの証明器は、ZKP 生成の複雑さをカプセル化し、開発者が C/C++、Rust などの高水準プログラミング言語を使用してビジネスロジックをコーディングできるようにし、カスタマイズされた回路を備えた ZKP 証明器を構築します。ZKP 生成ワークフローとドメイン固有言語 (DSL) についての深い理解が必要です。ただし、カスタマイズされた回路を備えた ZKP 証明器は、通常、zkVM ベースの証明器と比較して、より優れたパフォーマン

スを達成できます。ZKP 証明者を使用すると、DePIN 開発者は強力な ZKP テクノロジーを活用してトラストレスなオフチェーンコンピューティングを実行できるようになります。

W3bstream は、主要な zkVM/zkWASM プロジェクト (Risc0 [28]、Succinct SP1 [29]、Nexus [30]、zkWASM [31] など) や一般的な DSL (Circom [32] など) を段階的にサポートする予定です。Halo2 [33]、ZoKrates [34]、Noir [35]、Cairo [36] などを使用して、カスタマイズされた zk 回路を構築します。

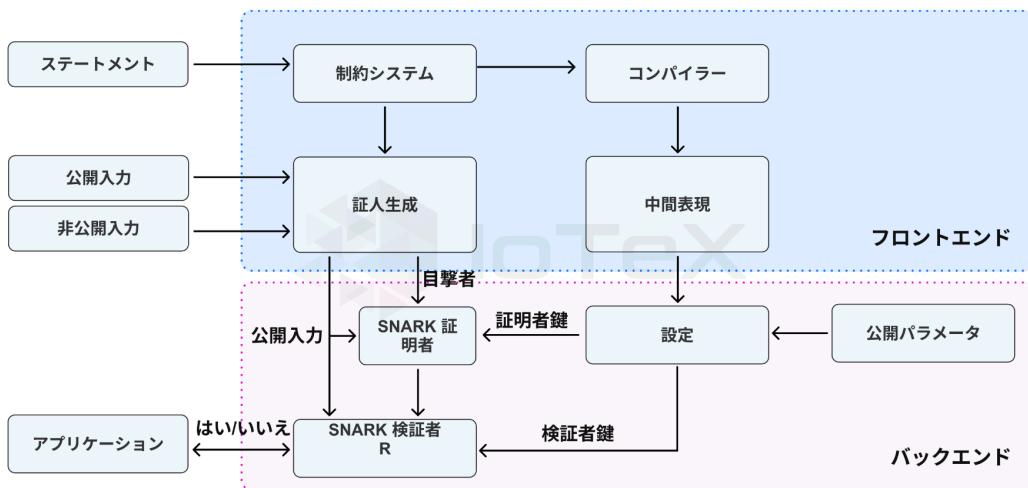


図 4.3: カスタマイズされた回路上に構築された SNARK ベースのアプリケーションのシステムアーキテクチャ

- **TEE Prover:** Confidential Computing Consortium (CCC) による定義によれば、信頼された実行環境 (TEE) は、次の 3 つの特性の一定レベルの保証を提供する専用のハードウェア (およびソフトウェア) 環境です。データの機密性: TEE 内でデータが使用されている間、権限のないエンティティはデータを表示できません。2) データの整合性: TEE 内で使用されているデータは、認可されていないエンティティによって追加、削除、または変更できません。3) コードの整合性: 権限のないエンティティは、TEE で実行されるコードを追加、削除、または変更できません。これらの顕著な

セキュリティ特性により、データとプログラムの両方の機密性と整合性が保証されるため、リモートパーティは TEE 対応ハードウェア プラットフォーム (例: Intel SGX、AMD-SEV、Arm CCA、AWS Nitro、NVIDIA H100) 上の計算結果を信頼できます。TEE ベースのシステムはセキュリティをハードウェアに根付かせるため、ユーザーはハードウェアが改ざんされていないこと、または検出できない形で壊れていることを信頼する必要があります。

TEE ベースのアプリケーションの典型的なシステム アーキテクチャを図 4.4 に示します。これは、TEE ベースのハードウェア プラットフォームのリモート認証メカニズムに依存しています。リモート構成証明は、一方の当事者 (検証者) が、信頼されていない可能性があるリモートピア (検証者) の信頼性を評価するプロセスです。認証の目的は、認証者のソフトウェアとデータの状態に関する本物の正確かつタイムリーなレポートを取得することによって、検証者が認証者の信頼性を確信できるようにすることです。構成証明サービスを利用すると、実行環境 (ハードウェア、ソフトウェア、カスタム データなど) の暗号測定を含む構成証明レポートを取得できます。

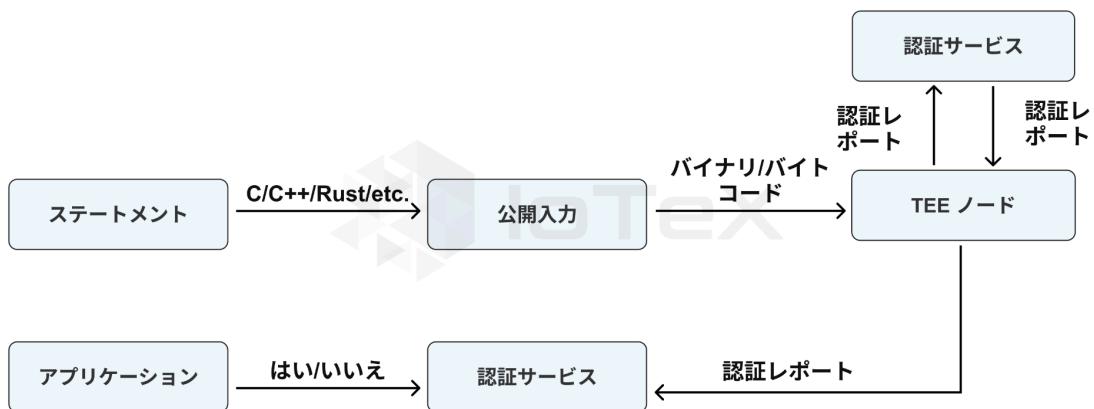
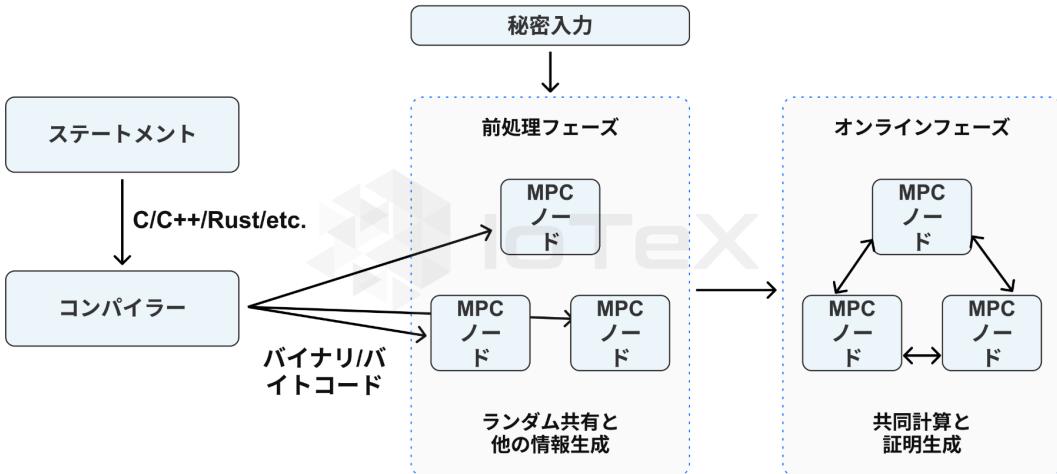


図4.4: TEEベースのアプリケーションのシステムアーキテクチャ

TEE 証明者は、特定の TEE プロバイダーの一般的な開発フローに従うことで実装できます。TEE 証明者は、DePIN 開発者が最先端の機密コンピューティング技術を利⽤して、プライバシーを保護するオフチェーンコンピューティングを実行できるようにします。W3bstream は、Intel SGX [37]、Intel TDX [38]、AMD SEV [39]、AMD SEV-SNP [40]、AWS Nitro [41] などの主要な TEE ベースのハードウェアプラットフォームの開発フローを段階的にサポートします。、アームCCA[42]など。

- **SMPC Prover:** MPC は、分散データ上でプライバシーを保護しながら共同計算を行うための技術のコレクションを表し、以下のことを明らかにします。計算結果。さまざまなセキュリティの仮定と脅威モデル (たとえば、半正直な敵対者、悪意のある敵対者、秘密の敵対者) を考慮すると、SMPC プロトコルは少なくとも 3 つの特性、すなわち入力プライバシー、入力の正確性、および独立性を満たさなければなりません。前処理モデルに基づいて構築された SMPC ベースのアプリケーションの典型的なシステム アーキテクチャを図 4.5 に示します。

図4.5: SMPCベースのアプリケーションのシステムアーキテクチャ



SMPC 証明者は、特定の SMPC プロトコル (SPDZ など) の一般的な開発フローに従うことで実現できます。ただし、効率的な方法で公的検証を実現することは、現在も研究の方向性として継続されています。

- **Bring Your Own Prover (BYOP):** BYOP は、特定の DePIN プロジェクトに合わせて最適化された証明者を展開したり、DePIN のコンテキストで新しい効率的な検証可能な計算技術を探索したりする DePIN 開発者に優れた柔軟性を提供します。

4.1.2 ZKPに関する社内イノベーション

マルチスカラー乗算 (MSM) は、多くのゼロ知識証明システムの中核コンポーネントの 1 つであり、これらのスキームにおける証明生成の主なパフォーマンスのボトルネックです。MSM を高速化するための主要な戦略の 1 つは、事前計算を利用することです。いくつかのアルゴリズム (Pippenger [11, 12] や BGMW [13] など) とその変形がこの方向で提案されています。私たちの最近の研究 [15] では、CHES 2023 [14] で Luo, Fu, Gong によって提

案された最近の事前計算ベースの MSM 計算手法を再検討し、そのアプローチを一般化します。特に、最適なバケットの一般的な構造を提示しました。この改善により、約 15% ~ 40% のパフォーマンス向上が得られ、理論分析と実験の両方で検証されています。また、 $j = 0$ の橙円曲線上の高速準同型性を使用してバケットに適した記録を導入し、すでに最適化されている LFG アルゴリズムと比較して、パフォーマンスをほとんど犠牲にすることなく、ストレージ要件を 3 で割りました。

4.2 W3bstream ワークフロー

4.2.1 証明者のオンボーディングと管理

証明者のオンボーディングは ioID に基づいており、セクション 5.2.2 - ioID の登録とバインディングで説明されているプロセスに従います。オンチェーンのフリート管理契約は、タスクのスケジュール設定とすべての証明者ノードのライフサイクルの追跡を担当します。各証明者ノードは、「ビジー」、「アイドル」、または「オフライン」のいずれかのステータスになり、ノードのステータスはフリート管理契約で継続的に更新されます。W3bstream エクスプローラーを使用して、すべての証明者ノードのステータスを確認できます。

4.2.2 ワークフロー

モジュラー DePIN インフラストラクチャでは、W3bstream はセクションで説明されている複数の証明者を特徴とするオフチェーン コンピューティング層 (OCCL) の実装です。

4.1. W3bstream は、データ可用性レイヤー (DAL) に保存されたデータに対してプロジェクト固有のビジネス ロジックを実行し、有効性証明 (ゼロ知識証明、証明レポートなど) を生成できる、分散型の異種証明者プールです。.) 実行された計算。W3bstream は、モジュール式

DePIN インフラストラクチャのステートレス コンピューティング コンポーネントとして機能し、以下の図 4.6 に示す高レベルの OCCL ワークフローに従います。

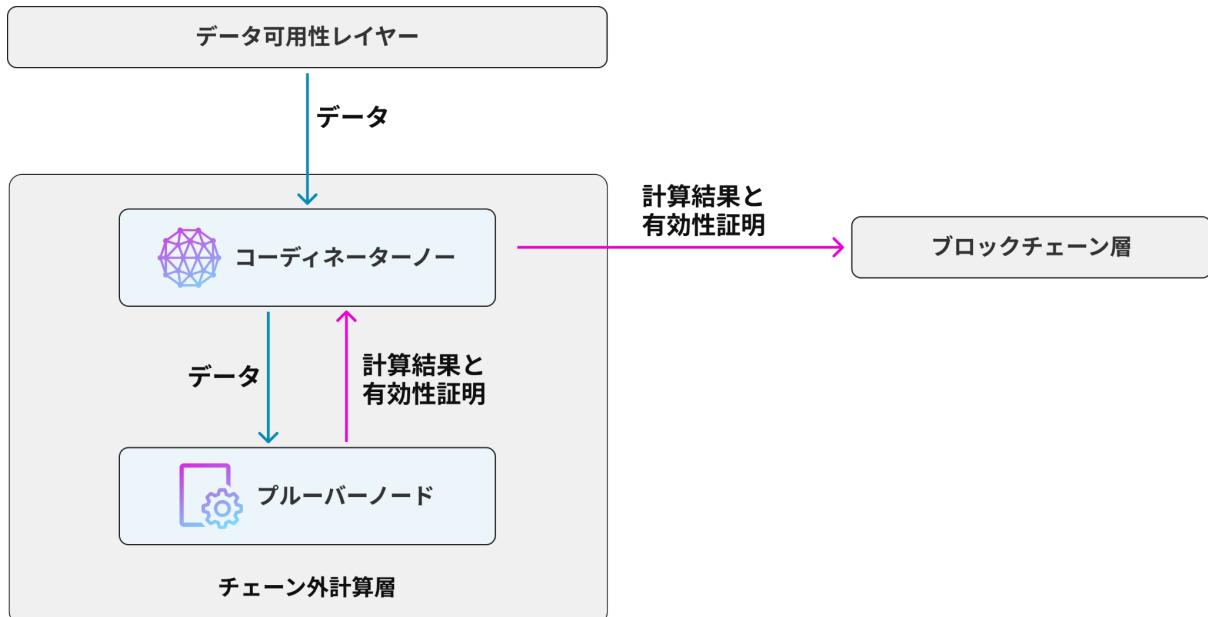


図4.6: オフチェーンコンピューティング層の高レベルワークフロー

1. オフチェーンコンピューティングレイヤーのコーディネーターノードは、DePIN プロジェクトの構成に基づいて、データ可用性レイヤーからデータを取得します。
2. オフチェーンコンピューティングレイヤーのコーディネーターノードは、DePIN プロジェクトの構成の基盤ついで、データ可用性レイヤーからデータを取得します。
3. 証明ノードは、DePIN プロジェクトによって指定された計算を実行し、計算結果と対応する有効性証明を生成します。
4. 計算結果と妥当性証明がコーディネーターノードに返されます。

5. コーディネーターノードは、計算結果と有効性の証明をスマートコントラクトに送信し、さらに処理します。

証明がオンチェーン上で正常に検証されると、計算結果は信頼され、DePIN プロジェクトの dApp によって使用されるようになります。

4.3 DePIN検証とオフチェーンAI

W3bstream で利用できる包括的な証明スイートにより、開発者は幅広い DePIN アプリケーションにおいてレイヤー 1 ブロックチェーンへのオフチェーン計算の整合性を証明できます。特に、開発者は特定のアプリケーションに最も適した検証可能な計算手法を選択できます。

4.3.1 DePIN認証

a16z の Guy Wouillet 氏が指摘しているように [43]、DePIN の成功は、中央機関を必要とせずに地理的に分散したサービスノードの信頼できる検証を保証するという極めて重要な課題に対処するかどうかにかかっています。DePIN 検証の現在の技術は、信頼できるハードウェアベースのアプローチ、統計的アプローチ、および有効性証明ベースのアプローチの 3 つのカテゴリに大まかに分類できます [44]。各検証アプローチにはそれぞれ長所と短所があり、実際には複数のアプローチの組み合わせが必要になる場合があります。W3bstream は、さまざまな DePIN プロジェクトがプラットフォーム上で検証アルゴリズムを開発し、その後更新することを容易にします。これらの検証アルゴリズムは、Rust、Golang、C++などの高水準プログラミング言語で記述できます。W3bstream で提供される証明器の 1 つを使用することで、DePIN 検証アルゴリズムの信頼性を保証できます。

4.3.2 オフチェーンAI

DePIN アプリケーションは、さまざまな業界分野にわたる AI トレーニングと推論の新たな機会を解き放ちます。一方で、DePIN アプリケーションは、信頼できる方法で大量の実世界データを Web3 に取り込むことができるため、AI モデルの精度が大幅に向上する可能性があります。一方、DePIN アプリケーションは、世界規模で AI のトレーニングと推論のためにコンピューティングリソースとストレージリソースを効果的に編成できます。ただし、AI アプリケーションは多くの場合、大量の計算を必要とするため、オンチェーンでの導入には大きな課題が生じます。W3bstream を使用すると、開発者はオフチェーン AI 計算を実行し、同時に計算プロセスの信頼性を確保できます。ゼロ知識証明はオフチェーンコンピューティングに強力な統合保護を提供できますが、AI (ZKML など) にゼロ知識証明を適用すると、検証不可能な AI 計算と比較すると、簡単に 10,000 倍から 100,000 倍のオーバーヘッドが発生する可能性があります。^{45]} 開発者は、ZKP 証明器を使用する代わりに、W3bstream でのオフチェーン AI 計算のために、より効率的な TEE 証明器に切り替えることができます。Arm の Veracruz フレームワークと AWS の Nitro エンクレーブに基づいて構築された私たちの最初の研究 [7, 8] は、非常に有望な結果をいくつか示しました。

第5章

ioID - DePIN 用の統一 ID システム

DePIN アプリケーションには、さまざまなシステム参加者間の広範なオンチェーン(つまり、ステーキング、資産転送、融資など)およびオフチェーン(つまり、個人からマシンへ、およびマシンからマシンへ)の相互作用が含まれます。モジュラー DePIN インフラストラクチャのアイデンティティ層は、さまざまなエンティティの関係を管理し、エンティティ間の安全なやり取りを確保するために不可欠なコンポーネントです。結果として、オンチェーンとオフチェーンの両方の相互作用の要件を満たすことができる統合 ID レイヤーを設計することは、DePIN アプリケーションにとって非常に望ましいことです。

5.1 オンチェーンとオフチェーンのアイデンティティ

5.1.1 オンチェーンアイデンティティ

オンチェーン ID の主な目的は、暗号資産の所有権を証明し、転送、ステーキング、融資などのさまざまな暗号資産関連操作を実行することです。外部所有アカウント (EOA) またはスマートコントラクトのブロックチェーンアドレスERC-4337 [25] で指定されているウォレット (SCW) は、この目的に適しています。特に、任意の検証ロジックを許可する SCW は、ブロックチェーントランザクションの複雑さ(署名検証、ノンス増加、ガス支払い、チェーンの互換性など)を抽象化し、エンドユーザーにとってブロックチェーンとの対話をより直観的にすることができます。追加の属性(イベントへの参加、提案投票など)は、非代替トークン (NFT)

[26] またはソウルバウンドトークン (SBT) を介してオンチェーン ID (つまり、ブロックチェーンアドレス) に関連付けることもできます。[27]。これらの属性は、特定の dApps (トークンのエアドロップなど) で必要になる場合があります。

5.1.2 オフチェーンアイデンティティ

DePIN アプリケーションでは、信頼できる人とマシン、マシンとマシンの関係を確立するためには、オフチェーンのアイデンティティが必要です。アイデンティティを公開鍵にバインドするデジタル証明書 (X.509など) は、集中型システムで信頼を実現するために広く使用されていますが、自己主権アイデンティティ (SSI) [48] は、分散型環境で 2 つのエンティティ間の通信を保護するための有望なアイデンティティソリューションを提供します。図 5.1 に示すように、SSI は、分散識別子 (DID) [49]、検証可能な資格情報 (VC) [51]、および DIDComm メッセージング [50] という 3 つの主要な柱で構成されています。分散型システムの各参加者 (つまり、人またはマシン) が検証可能なデータレジストリ (ブロックチェーンなど) に DID を登録すると、2 つのエンティティは安全な通信チャネルを確立し、DIDComm メッセージを交換して相互に認証できます。VC は、特定のエンティティ (つまり、VC 発行者) によって追加の ID 属性が証明される必要がある場合に便利です。

5.2 ioID の設計

ioID は、ブロックチェーンウォレットアドレス (外部所有アカウント (EOA) またはアカウント抽象化 (AA) ウォレット) をオンチェーン ID として、DID をオフチェーン ID として利用し、IoTeX によって設計された統合 ID システムです。DePIN アプリケーションの参加者間のオン

チェーンおよびオフチェーンのデジタル関係。汎用の ID システムとして、私たちは ioID が次のようなことを実現できることを想定しています。

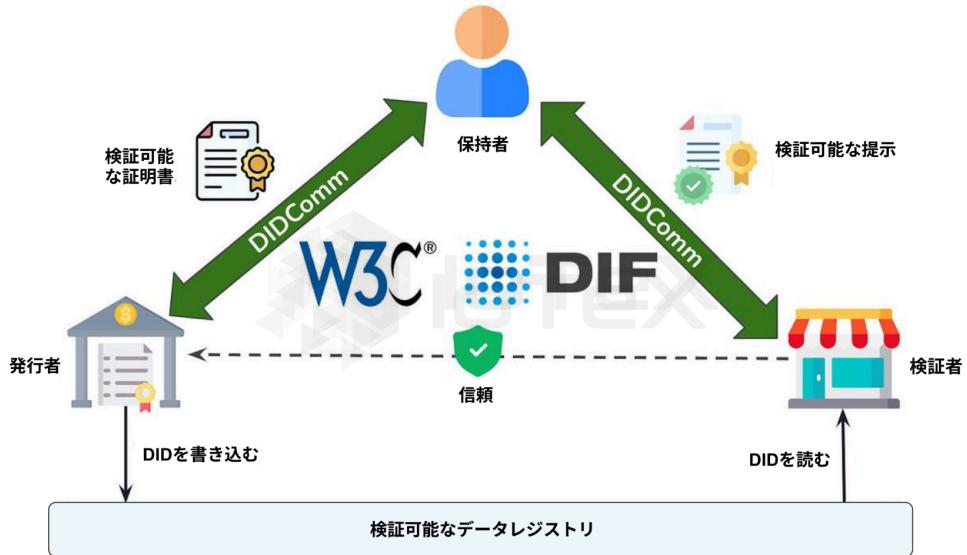


図5.1: SSIの3つの主要な柱

図5.2に示すように、DePINモジュラーインフラストラクチャのさまざまなレイヤーで利用できます。

5.2.1 デバイス上でのioID生成

DePINデバイスは、IoTeXのioConnect SDK [16]を統合することにより、デバイス内でDIDと対応するDIDドキュメントをオンザフライで生成できます。モジュール式DePINスタック内の特定の集中型または分散型レイヤーの操作をサポートするために展開されたDePINノードの場合、ノードオペレーターはコマンドラインインターフェイス(CLI)を使用してDIDとDIDドキュメントを生成できます。組み込みDePINデバイスの場合、メーカーはioConnect SDKをデ

バイスのファームウェアに統合し、ユーザーがデバイスからDIDとDIDドキュメント(シリアルポート経由など)を読み取れるようにすることができます。

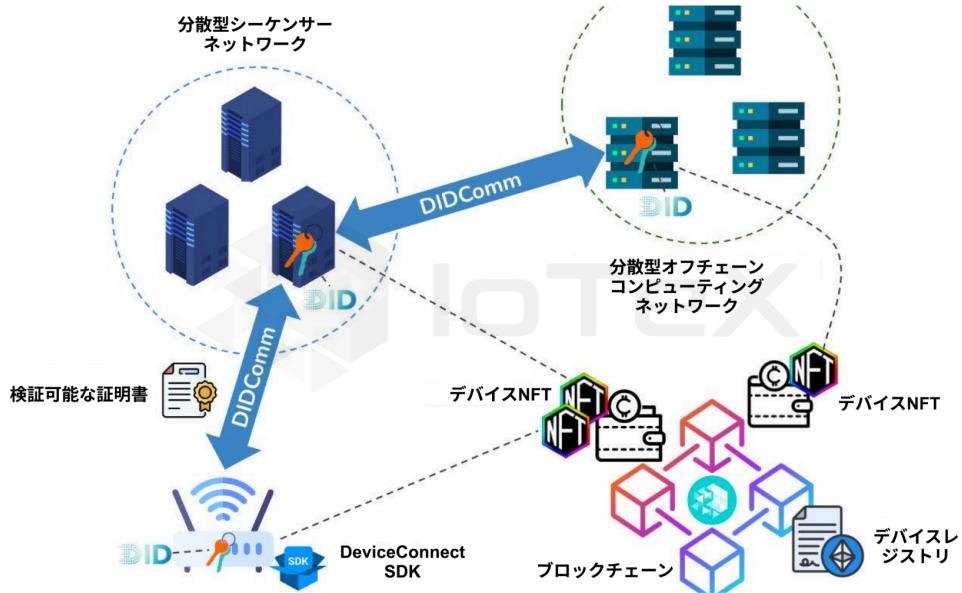


図5.2: ioIDアイデンティティシステムの概要

5.2.2 デバイス上でのioID生成

DePIN デバイスの所有者は、Web ポータル (IoTeX の MachineFi ポータルなど) を介してデバイスをオンボードできます。オンボーディング プロセスを図 5.3 に示します。

1. デバイス所有者はまずMetamaskを使用してWebポータルにログインします。
2. デバイス所有者は、Web ポータルで最小トークン デポジット (例: 10 IOTX トークン) を行います。これらのトークンは、デバイスのオンボーディング プロセス中にガス料金を支払うために使用されます。
3. デバイス所有者は、DePIN デバイスの DID と DID ドキュメントを取得します。

- a) DePINノードの場合、デバイス所有者(ノードオペレータ)はローカルまたはリモートでノードにログインし、CLIを使用してノード上にDIDと対応するDIDドキュメントを生成する必要があります。
- b) 埋め込み型DePINデバイスの場合、デバイス所有者は
- i. i. デバイスをUSB経由でPCに接続します。

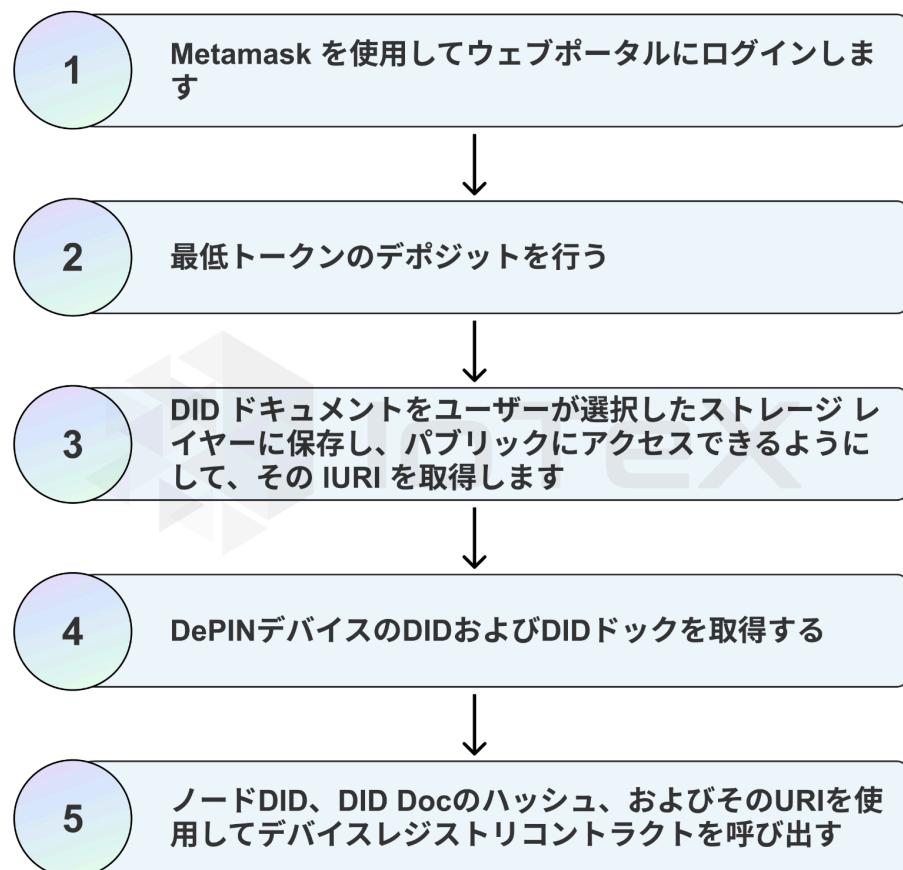


図5.3: DePINデバイスを導入するマイナーの道のり

ii. ii. Web ポータルの [デバイス DID および DID ドキュメントの読み取り] ボタンをクリックして、シリアル ポート経由でデバイスの DID および DID ドキュメントを取得します。

4. デバイス所有者は、集中型または分散型のストレージ層プロバイダー AWS S3、IPFS など)を選択し、DID ドキュメントを保存し、パブリックにアクセスできるようにして、URI を取得します。

5. デバイス所有者は、デバイスの ii. Web ポータルの「デバイス DID と DID ドキュメントの読み取り」ボタンをクリックして、シリアル ポート経由でデバイスの DID と DID ドキュメントを取得します。図5.3: DePINデバイスを導入するマイナーの道のり DID、DID ドキュメントのハッシュ、および DID ドキュメントの URI。

デバイスのオンボーディング プロセスが正常に完了すると、DePIN デバイスの所有者は、自分のブロックチェーンウォレットにデバイス NFT が表示され、DePIN デバイスのオンチェーン所有権が表れるのを確認できます。

5.2.3 安全なマシン間インターフラクション

デバイスのオンボーディング プロセス中に DePIN デバイスの DID がオンチェーンで登録されると、標準化された DIDComm メッセージング プロトコルに基づいて、ネットワーク内の他のエンティティと安全なオフチェーン通信を実行できるようになります。

5.3 DePINプロジェクトへのioIDの統合

DePIN プロジェクトでは、ioID モジュールを使用する前にいくつかの設定を完了する必要があります。

5.3.1 ioIDのスマートコントラクト 5

ioID スマートコントラクトスイートは、IoTeX ブロックチェーン上の分散型 ID 管理のための堅牢なフレームワークを提供します。これらのコントラクトは、IoTeX エコシステム内での ID 管理とインタラクションのための堅牢なフレームワークを総合的に提供します。

- **DePIN プロジェクトレジストリ:** DePIN プロジェクトレジストリは、すべての DePIN プロジェクトを管理する NFT ベースのレジストリです。これにより、各プロジェクトがネットワーク内で一意に識別され、認証されることが保証されます。
- **ioID NFT Contract:** ioID NFT コントラクトは、IoTeX ブロックチェーン上の分散型 ID 管理のための ioID フレームワークの重要な部分です。これはプロジェクトレジストリによって直接管理され、デバイスの一意の ioID トークンの作成と割り当てを担当します。これには、デバイスをプロジェクト ID および所有者にリンクし、ERC6551 標準に従って関連するウォレットアドレスを生成することが含まれます。
- **ioID Store:** ioID Story は、すべてのプロジェクトにわたる ioID のアプリケーションとアクティブ化の管理を担当します。ID 管理アプリケーションのライフサイクルを処理し、ID が正しく設定および維持されるようにします。
- **ioID レジストリ:** ioID レジストリコントラクトは、デバイスをオンチェーンで登録し、ioID をアクティブ化するために使用されます。また、DID リゾルバーとしても機能し、

異なるプロジェクト間でデバイス ID を検証するための信頼性の高い手段を提供します。

5.3.2 デバイスNFTコントラクトの展開

DePIN プロジェクトを IoTeX ioID モジュールと統合するには、プロジェクト所有者は、プロジェクト内の各デバイスをトークン化する「デバイス NFT」コントラクトをデプロイすることから始めます。DePIN プロジェクトのデバイス NFT を所有するユーザーは、物理デバイスの新しい ioID ID を登録し、それを自分のブロックチェーンウォレットにバインドする権利があります。デバイスに新しい ioID が登録されると、ioID NFT が所有者のウォレットに鑄造され、対応するデバイス NFT が ioID の ERC-6551 ウォレットに転送されます。このプロセスにより、ioID が効果的に「アクティブ化」され、物理デバイスがそのデジタル ID とブロックチェーン上の所有者にリンクされます。

5.3.3 DePIN プロジェクトの登録

ioID ID を使用する予定の DePIN プロジェクトは、必要な金額を支払って一定数の ioID を申請する必要があります。ioID をリクエストできるのは、IoTeX ブロックチェーンに登録された DePIN プロジェクトのみです。プロジェクト所有者は、直接スマートコントラクトを呼び出しか、IoTeX コマンドライン インターフェイス (ioctl) を使用して DePIN プロジェクトを登録できます。トランザクションが完了すると、IoTeX ブロックチェーン上の DePIN プロジェクト ID を表す特定のトークン ID を持つプロジェクト NFT を受け取ります。

5.3.4 デバイスNFT契約の設定

DePIN プロジェクトを登録した後、次のステップは、ioID ストアでそのプロジェクトのデバイス NFT コントラクトを設定することです。このコントラクトは、デバイスがプロジェクトの ioID を登録しようとする前に設定する必要があります。プロジェクト所有者は、直接スマートコントラクトを呼び出すか、IoTeX コマンドラインインターフェイス (ioctl など) を使用してこのステップを完了できます。

5.3.5 ioIDのリクエスト

プロジェクト所有者は、必要な量の IOTX トークンを支払って ioID を申請する必要があります。この量は、要求された ioID の数によって決まります。プロジェクト所有者は、直接スマートコントラクト呼び出しを行うか、IoTeX コマンドラインインターフェイス (つまり、ioctl) を使用して ioID を要求できます。トランザクション後、要求された ioID の数が DePIN プロジェクトに関連付けられます。

5.3.6 デバイスの登録

デバイス NFT コントラクトを設定し、DePIN プロジェクト用に一定数の ioID をリクエストすると、物理デバイスを ioIDRegistry コントラクトに登録することで、プロジェクト用にアクティブ化できるようになります。このプロセスはデバイス所有者によって実行され、デバイス所有者のアカウントに新しい ioID NFT が作成され、デバイスの DID とデバイス NFT にバインドされます。

第6章

ioConnect - デバイスの抽象化を強化する

ためのユニバーサル組み込み SDK

DePIN アプリケーションには、さまざまな能力と機能を備えた多様なハードウェア デバイスが含まれます。モジュラー DePIN インフラストラクチャにおけるハードウェア抽象化レイヤー (HAL) の主な目的は、さまざまなスマートデバイス (大小を問わず) の複雑さと異質性を抽象化し、集中型または分散型の接続レイヤー (図 6.1 に示すように、CL) を安全な方法で保存します。難しい問題は、デバイスメーカーがデバイスを DePIN バックエンドに簡単に接続できるようにするユニバーサル組み込み SDK を設計することです。実際には、ioConnect SDK は、一般的なマイクロコントローラファミリ (例: ESP32、Arduino、STM32 など)、シングルボードコンピュータ (例: Raspberry Pi、ODROID、Rock Pi など)、およびスマートフォン (例: Android および iOS) が非常に望ましいです。



図6.1: HALとCL間の安全な接続

6.1 接続オプション

6.1.1 集中接続レイヤーへの接続

スマートデバイスを集中接続層 (クラウドベースの IoT ゲートウェイなど) に接続することは、従来の IoT 業界で広範囲に調査されており、その技術の成熟度により、かなりの数の初期段階の DePIN プロジェクトで採用されています。デジタル証明書 (X.509 など) は、スマートデバイスと集中接続層の間の安全な通信を確保するためによく利用されます。例としてクラウドベースの IoT ゲートウェイ (AWS IoT Core [46] など) を使用すると (図 6.2 を参照)、ユーザーはまずクラウド内にデジタルツインを作成し、デバイス証明書を生成できます。証明書がスマートデバイスにインストールされると、クラウドベースの IoT ゲートウェイとの安全な TLS 接続を確立できます。その後、デジタルツインはスマートデバイスに代わってクラウド内の他のサービスと対話します。

集中接続層は、デバイスの接続と管理を簡素化する一方で、DePIN アプリケーションの单一障害点となるため、将来の DePIN プロジェクトでは分散接続層の採用を真剣に検討する必要があります。



図6.2: AWS IoT Coreを使用したデバイスのオンボーディング

6.1.2 分散接続層への接続

分散型接続レイヤーは DePIN アプリケーションに対してより堅牢なネットワーク接続を提供しますが、スマートデバイスを接続すると、次のような多くの技術的な課題が生じます。

- スマートデバイスは、集中型の証明機関 (CA) やデジタル証明書に依存せずに、分散型接続レイヤー内のノードに安全に接続するにはどうすればよいですか？
- スマートデバイスは、分散型接続レイヤー内のノードとどのように相互認証できるでしょうか？
- スマートデバイスはどのようにしてネットワーク内のノードと安全なチャネルを確立できるのか？ 集中型接続レイヤー？

前述の技術的な課題に対処するために、DePIN デバイスは、このような分散化された設定で使用できる新しいテクノロジーとプロトコルを実現する必要があります。

6.2 DePINデバイス用のユニバーサル組み込みSDKを構築するための設計上の考慮事項

幅広いスマートデバイスを適切に統合された接続レイヤーに接続する際の潜在的な課題により、DePIN デバイス用のユニバーサル組み込み SDK の開発に向けて、次の設計要件が生じました。

- SDK は、一般的なハードウェアチップセットとプラットフォーム（マイクロコントローラ、シングルボードコンピュータ、スマートフォンなど）に対応する必要があります。
- SDK は、DePIN デバイスメーカーによって自社のデバイスに簡単に統合される必要があります。
- SDK は、DePIN デバイスが高度なセキュリティ機能（セキュアエレメント、暗号化アクセラレーターなど）を使用できるようにする必要があります。
- SDK は、DePIN デバイスが分散環境で他のエンティティ（人やマシンなど）と信頼関係を確立できるようにする必要があります。

これらの設計要件により、Arm の PSA 認定暗号 API や自己主権型アイデンティティ (SSI) などの新しいテクノロジーや、階層化された SDK 設計方法論を探求するようになりました。

6.2.1 Arm の PSA 認定暗号 API

ArmのPSA認定暗号API[47]は、幅広いハードウェアプラットフォーム上で暗号操作や鍵管理サービスにアクセスするための標準化された統一インターフェースを定義しています。開発者は、ターゲットハードウェアプラットフォームで利用可能な暗号ソフトウェア/ハードウェアドライバーをロードすることで、図6.3に示すように、PSA暗号APIを通してすべてのセキュリティ関連機能に簡単にアクセスできます。

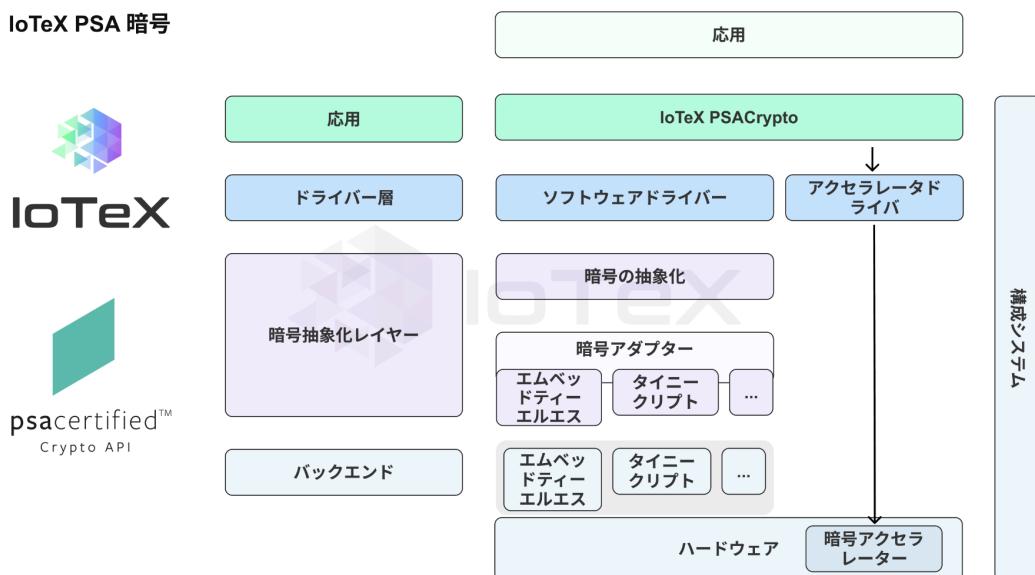


図6.3: DePINデバイスにおけるIoTeXのPSACryptoライブラリの使用

Arm の PSA 認定暗号 API を DePIN デバイスに統合すると、DePIN デバイスのセキュリティが強化される可能性があり、それによって DePIN アプリケーションで増加する詐欺リスクを効果的に軽減できます。

6.2.2 自己主権アイデンティティ(SSI)

分散型識別子 (DID) [49]、検証可能資格情報 (VC) [51]、DIDComm メッセージング [50]などの自己主権アイデンティティ (SSI) [48] 技術は、デジタル ID の管理を従来の ID プロバイダーから個人に移します。そして、豊かなデジタル関係を形成する人、組織、物事の基盤を築きます。図 6.4 に示すように、分散型設定では、SSI は、サードパーティの集中型または連合型 ID プロバイダーに依存せずに、信頼できる個人とマシンおよびマシンとマシンの関係を確立するための有望なソリューションを提供します。

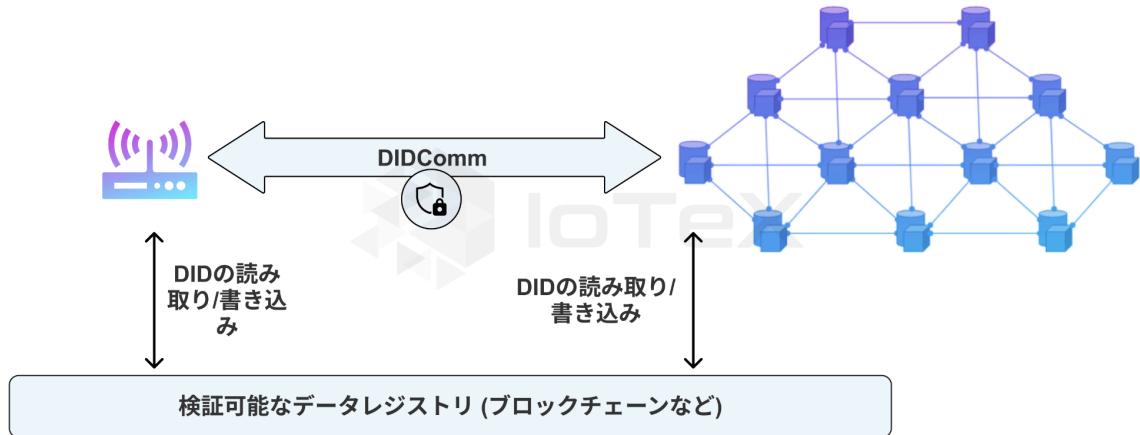


図6.4: 分散環境におけるSSIベースの通信

6.3 実装仕様

ioConnect [16]は、IoTeXがDePINデバイスを強化するために特別に設計したユニバーサル組み込みSDKです。幅広いスマートデバイスとアプリケーション要件をサポートするために、SDKはSDKコアとプラットフォーム適応層(PAL)で構築されています。

6.3.1 ioConnect SDK コア

ioConnect のコアは、図 6.5 に示すように 4 つのレイヤーで構成されています。下の 2 つのレイヤーは Arm の PSA 認定暗号 API 仕様 v1.1 を実現し、上の 2 つのレイヤーは SSI の 3 つの主要な柱 (つまり、DID、VC、および DIDComm) を実装します。SSI で必要なすべての暗号化操作は、PSA 暗号 API 呼び出しを通じて実行されます。

ioConnect SDK コアはハードウェア プラットフォームから独立しており、DePIN デバイス上の特定のコンポーネント/リソースにバインドされないように注意してください。

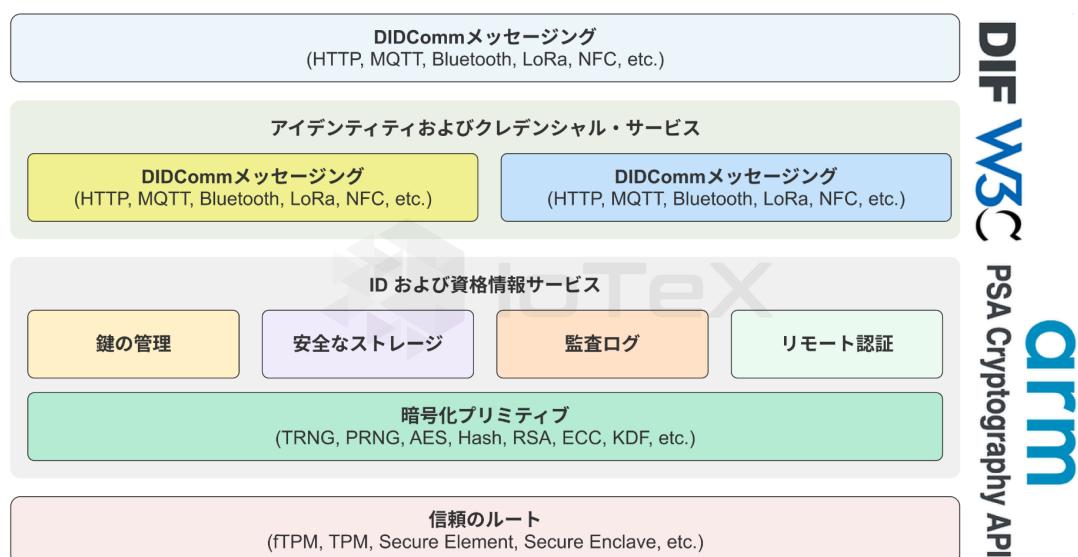


図6.5: ioConnect SDKコア

6.3.2 DePINデバイスの互換性

幅広い DePIN デバイスに対応するために、ioConnect SDK 全体は、図 6.6 に示すように階層化された設計手法を採用しています。一方では、コアにはハードウェアに依存しない仕様 (例: SSI、PSA 暗号化 API など) の実装が含まれており、プラットフォームアダプションレイ

ヤー (PAL) は、さまざまな組み込みシステムおよびプラットフォーム間の差異 (例: コンパイアルなど) に対処します。ルール、コーディング規約、フレームワーク設計など)。

PAL の導入により、開発者は、わずか 300 ~ 500 行のコードで別の PAL コンポーネントを開発するだけで、新しいハードウェア サポートを簡単に追加できるため、DePIN デバイスの互換性問題に効果的に対処でき、DePIN デバイスメーカーの統合の複雑さが大幅に軽減されます。

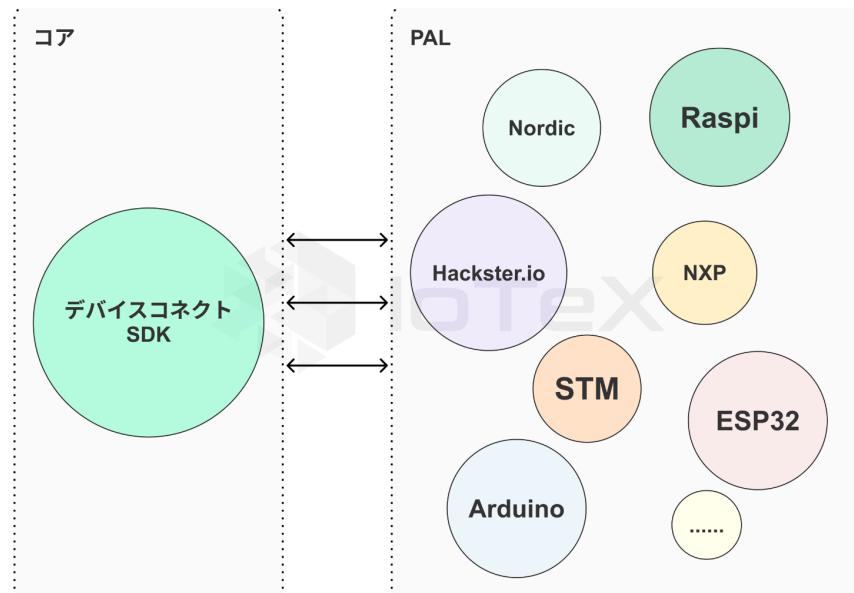


図6.6: ioConnect SDKの階層化アーキテクチャ

第7章

ioDDK - 自己主権型 DePIN アプリ チェーンの有効化

7.1 設計の根拠

IoTeX L1 上の DePIN プロジェクトでアプリケーション固有の L2 を有効にする理由は、いくつかの説得力のある要因によって決まります。

- 第一に、アプリケーション固有の L2 は、独自のトークンノミクス、カスタマイズされたユーザー エクスペリエンス (ウォレットやブラウザなど)、およびカスタマイズされたガバナンス構造の導入を可能にするため、DePIN プロジェクトにとって非常に重要です。このカスタマイズは、ブロックチェーンを最適化して各 DePIN アプリケーションの特定のニーズとシナリオをスケーラビリティで満たし、各プロジェクトがその可能性を最大限に発揮できるようにするために不可欠です。
- さらに、多くの DePIN プロジェクトには、独自のブロックチェーン インフラストラクチャを構築および維持するために必要な専門知識と資金が不足しています。

現時点では、IoTeX L1 は、社内の Randomized Delegated Proof-of-Stake (Roll-DPoS) コンセンサスプロトコルを通じて、120 人以上のグローバルに分散されたデリゲート (つまり、バリデータ) のプールによってセキュリティが確保されています [52]。IoTeX L1 の安全なプロッ

クススペースを活用することで、これらの DePIN プロジェクトは、ブロックチェーン開発に伴う重労働をすることなく、アプリケーション固有の L2 をシームレスに起動できます。

ioDDK は、図 7.1 に示すように、DePIN プロジェクトが自己主権アプリケーションチェーンをプロビジョニングし、同時に IoTeX L1 のセキュリティを継承できるようにするチェーン SDK です。バリデーターは、IoTeX L1 ブロックを検証して提案する一方で、DePIN アプリケーションチェーンからのトランザクションについても合意に達します。ブロックスペースをレンタルすることで、IoTeX L1 は、巨額の先行投資や技術的ノウハウを必要とせずに、カスタマイズされたソリューションを効率的に展開するために必要なリソースを DePIN プロジェクトに提供し、より活気に満ちた革新的なエコシステムを育成できます。

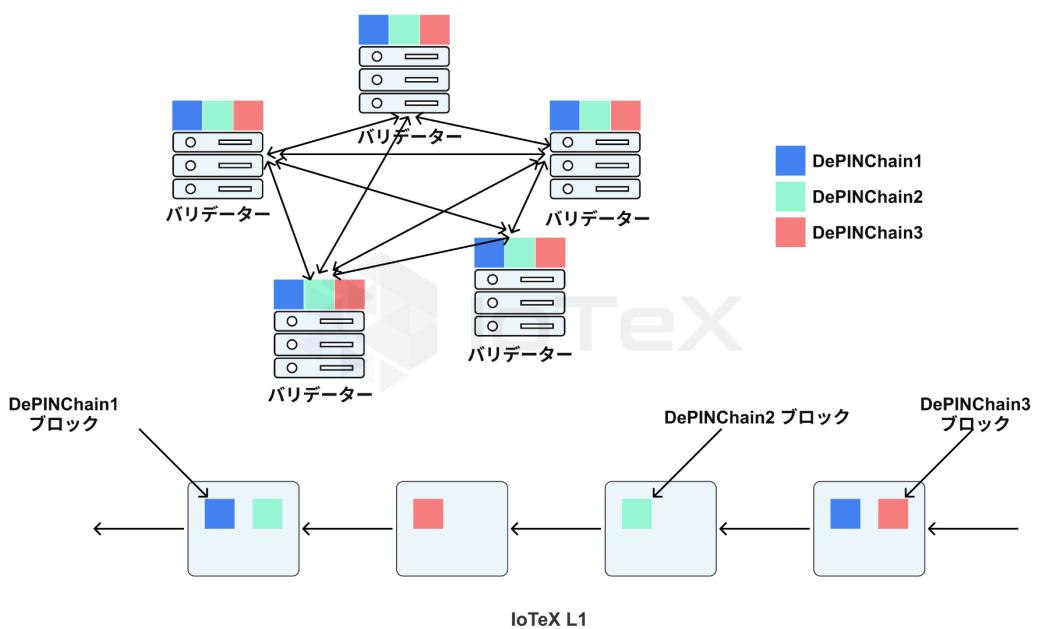


図7.1: IoTeX L1で保護された自己主権型DePINアプリチェーン

7.2 共有ブロックスペースとバリデーター

開発の複雑さを最小限に抑えるために、すべての自己主権型DePINチェーンは共有できる。IoTeX L1を使用したブロックスペースとバリデータ。3つの実装オプションがあります。図7.2に示すように、実際には考慮する必要があります。

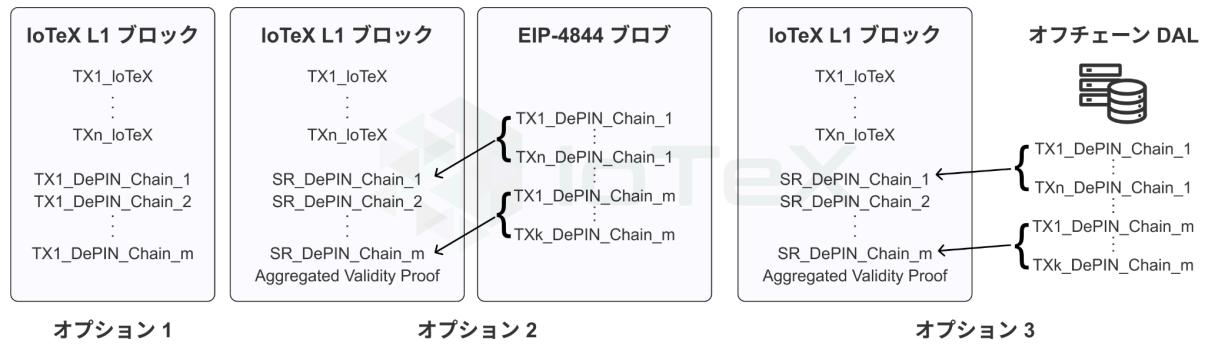


図7.2: 共有ブロックスペースとバリデーターの3つの実装オプション

オプション1 - すべてのトランザクションをIoTeX L1に保存する

このオプションでは、自己主権型 DePIN チェーンからのトランザクションと IoTeX L1 上のトランザクションが同じブロックスペースを共有し、すべてのトランザクションは IoTeX L1 のコンセンサスプロセスを経る必要があります。このアプローチにより、すべての自己主権型 DePIN チェーンが IoTeX L1 と同じセキュリティを実現できます。ただし、ブロック サイズの制限により、サポートできる DePIN プロジェクトは一定数に限られます。このアプローチを使用する資格のある DePIN プロジェクトを決定するには、分散型ガバナンスプロセスが必要になる場合があります。

オプション2 - EIP-4844 を使用して DePIN チェーントランザクションを保存する

このオプションでは、自己主権型 DePIN チェーンからのトランザクションは、EIP-4844 BLOB を使用して IoTeX L1 に一時的に保存されます。すべての自己主権型 DePIN チェーンの状態遷移の集約された有効性証明とともに、状態ルートは IoTeX L1 トランザクションと同じブロックスペースを共有します。集約された有効性証明は IoTeX L1 で検証され、自己主権型 DePIN チェーンのすべてのトランザクションを決済します。このようなロールアップベースのアプローチは、システムのスケーラビリティを効果的に向上させ、すべての自己主権型 DePIN チェーンが同時に IoTeX L1 のセキュリティを継承できるようにします。このアプローチを実現するには、W3bstream ネットワークの証明者の 1 つを利用する必要があることに注意してください。

表7.1: 3つの実装オプションの比較

	デピンチェーン トランザクション ストレージ	スケーラビリティ	W3bstream 必要	安全
オプション 1	オンチェーンブロック	低い	いいえ	高い
オプション 2	オンチェーンブロブ	高い	はい	高い
オプション 3	オフチェーン DAL	高い	はい	低/中

オプション3 - オフチェーンDALを使用してDePINチェーントランザクションを保存する

このオプションでは、自己主権 DePIN チェーンは、トランザクションを保存するためにオフチェーンのデータ可用性レイヤー (DAL) を選択できます。オプション 2 と同様に、状態ルートは、すべての自己主権 DePIN チェーンの状態遷移の集約された有効性証明とともに、IoTeX L1 トランザクションと同じブロックスペースを共有します。集約された有効性証明は IoTeX L1 で検証され、自己主権 DePIN チェーン上のすべてのトランザクションが決済されます。ただし、このアプローチでは、状態ルートは DAL によって IoTeX L1 にコミットされる必要があります。このような検証ベースのアプローチでもシステムのスケーラビリティを向上させることができます。セキュリティは特定の DAL の実装に依存します。このアプローチを実現するには、W3bstream ネットワーク内の証明者の 1 つを利用する必要があることに注意してください。

3つのオプションの比較

表 7.2 は、DePIN チェーントランザクションストレージ、スケーラビリティ、W3bstream 要件、セキュリティに関する上記 3 つの実装オプションの比較を示しています。

7.3 ioDDK コンポーネントと高レベルワークフロー

7.3.1 ioDDK コンポーネント

ioDDK は、DePIN プロジェクトが IoTeX L1 内の既存のデリゲート (バリデーター) とブロックスペースを活用して自己主権型 DePIN チェーンをホストできるようにするもので、次のコンポーネントで構成されています。

- チェーン構成: チェーン構成コンポーネントを使用すると、開発者は DePIN チェーンの特定のパラメータ (開始の高さ、トランザクションの種類、ブロックスペースの要件など) を構成できます。

- **チェーン展開:** チェーン展開コンポーネントを使用すると、開発者は IoTEx L1 のすべてのデリゲートにわたる DePIN チェーンの展開プロセスを管理できます。
- **チェーン エクスプローラー:** チェーン エクスプローラーコンポーネントを使用すると、DePIN プロジェクトだけでなく外部の関係者も DePIN チェーンのステータスと主要なメトリック（ブロックの高さ、TPS、トランザクションの詳細など）を監視できます。
- **チェーンコマンダー:** チェーンコマンダーは、DePIN チェーンの開発と管理を簡素化する一連のコマンドを提供するコマンドラインツールです。

7.3.2 高レベルワークフロー

DePIN プロジェクトが IoTEx L1 の共有ブロックスペースとバリデーターを使用して自己主権チェーンをプロビジョニングすることを承認されると（たとえば、分散型ガバナンスプロセスを介して）、プロジェクトは次のように ioDDK を使用できるようになります。

- 開発者は、ioDDK の「チェーン設定」機能を使用して、DePIN チェーン固有のパラメータの数を指定します。
 - **chainID:** 自己主権 DePIN チェーンを表すチェーン識別子が自動的に生成されます。
 - **トランザクションタイプ:** トランザクション内のさまざまなフィールド。
 - **最大トランザクション数:** IoTEx L1 ブロックで処理される DePIN チェーントランザクションの最大数。
 - **W3bstream 証明者:** W3bstream 証明者の選択。

- 開発者は、DePIN チェーンのトランザクション処理ロジックの Docker イメージを準備し、ioDDK の「チェーン デプロイメント」機能を使用して、IoTeX L1 のすべてのデリゲートに Docker イメージをデプロイします。

DePIN チェーン固有のトランザクション処理ロジックが IoTeX L1 デリゲートに展開されると、DePIN チェーントランザクションがそれに応じて処理されます。開発者は、ioDDK の「Chain Explorer」を使用して、プロビジョニングされた DePIN チェーンのステータスを確認できます。さらに、開発者は「Chain Commander」を使用して、いくつかのサポートコマンドを使用して DePIN チェーンを管理することもできます。

7.4 ブロックスペースをレンタルするためのマーケットプレイス

私たちは、ioDDK で構築された特定の DePIN L2 に合わせてカスタマイズされたブロックスペースを開発者が取引できるようにするブロックスペースマーケットプレイスを実装する予定です。この市場指向の戦略により、リソース割り当てがリアルタイムの需要に適応し、ネットワーク全体の効率が最適化されます。

取引可能なブロックスペースの導入は、IOTX トークンの有用性と流動性にも影響を与えます。たとえば、開発者は IOTX をステークまたはバーンして、一定量のブロックスペースを取得できます。トランザクションから得られる収益は、財務への資金提供やトークン供給の調整のためにバーンされるなど、複数の方法で配分できます。

7.5 IoTeX L1への影響

IoTeX L1 に共有ブロックスペースを導入することで、DePIN L2 プロジェクトの増大する需要を満たすように設計された多数の機能が実現します。

- 高速なブロックタイムとファイナリティ: DePIN L2 の主な要件の 1 つは、ユーザー エクスペリエンスを最適化するための高速なブロックタイムと素早いファイナリティです。現在、IoTeX L1 のブロック時間は 5 秒です。ただし、高パフォーマンスの DePIN プロジェクトのニーズを満たすために、このブロック時間を 2 秒に短縮することを目指しています。この削減により、L2 アプリケーションの応答性と効率が大幅に向上し、よりスムーズでユーザーフレンドリーなエクスペリエンスが保証されます。
- スループットの向上と分散化: De-PIN L2 の合計スループットは、IoTeX L1 ネットワーク内のすべてのバリデーターのコンピューター能力によって本質的に制限されます。これに対処するには、バリデーターの数を増やすことと、ネットワーク全体の分散化を改善することが重要です。バリデータープールを拡張することで、IoTeX L1 はより多くのトランザクション量をサポートし、より堅牢なセキュリティを提供できます。この機能強化により、成長するエコシステム内で信頼と安定性を維持するために不可欠な、より分散化された復元力のあるネットワークも促進されます。

上記の要件を満たすために、Proposer-BUILDER Separation (PBS) [53] の導入が計画されています。PBS は、もともとイスラエルの研究者によって提案された概念で、ブロックチェーン ネットワークの検閲耐性と全体的なパフォーマンスを強化するために設計されました。ブロック提案者とブロック構築者の役割を分離して、ブロック生成を最適化し、検証プロセスの公平性を確保します。

- ブロック提案者: ブロックチェーンの現在の状態とネットワークルールに基づいて新しいブロックを提案する責任を負います。彼らはトランザクションを収集し、ネットワークによって検証されるブロック提案を作成します。この役割は、おそらく現在のコンセンサス代表者によって果たされることになるでしょう。

- ブロックビルダー: ブロック構築に特化したエンティティで、アクトプールから最も価値のあるトランザクションを選択し、ブロックスペースの使用を最適化し、スループットを向上させることができます。構築したブロックを提案者に提出し、提案者はこれらのブロックを検証のためにネットワークに提案します。これは、IoTeX L1 ネットワークに導入される新しい役割です。ブロック構築に特化したエンティティで、アクトプールから最も価値のあるトランザクションを選択し、ブロックスペースの使用を最適化し、スループットを向上させることができます。構築したブロックを提案者に提出し、提案者はこれらのブロックを検証のためにネットワークに提案します。これは、IoTeX L1 ネットワークに導入される新しい役割です。De-PIN L2 からのトランザクションを含むパッケージトランザクションに専念します。

これらの役割を分離することで、さまざまなエンティティに責任を分散し、集中管理と検閲のリスクを軽減できます。これにより、ネットワーク容量が向上し、トランザクション処理時間が短縮されます。つまり、ビルダーはトランザクションの選択、最適化、さらにはシャーディングに集中でき、提案者はコンセンサスとブロックの確定プロセスを処理できるため、より効率的なブロック生成が可能になります。このアプローチにより、IoTeX L1 によって提供される共有ブロックスペースに基づく DePIN L2 が効率的かつ安全に動作し、特定のアプリケーションシナリオの要求を満たすことができます。

第8章

新しいロードマップ[°]

IoTeX 2.0 は、現在から 2026 年までに構築する予定の多数のコンポーネントのコレクションです。ロードマップは、下の図 8.1 に示されています。リストされているコンポーネントの多くは、ガバナンス提案と投票に依存しているため、変更される可能性があることに注意してください。

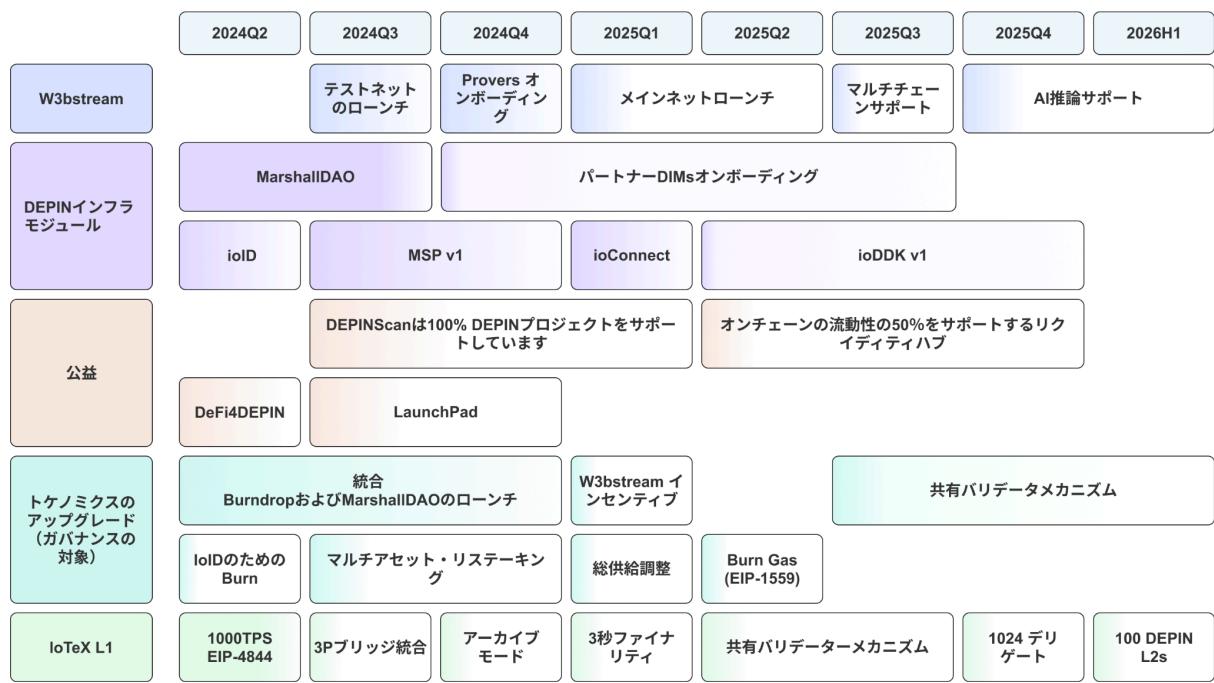


図8.1: IoTeX 2.0 ロードマップ[°]

第9章

結論

IoTeX 2.0 は、IoTeX ネットワークの新たなビジョンを提示しながら、その発端となった中核原則を維持しています。IoTeX は当初から、個人が自分のデバイスを所有し、制御できる未来、およびこれらのデバイスが生成するデータと価値を所有できる未来を思い描いていました。IoTeX は、現実世界のリアルタイムデータのハブとなり、超知能 AI ネットワークを実現することを目指しています。このネットワークは人間の知能を超えるだけでなく、現実世界をリアルタイムで反映する正確で信頼性の高いデータを活用します。この変化は、究極の真実と意思決定力が、私たちの物理的環境の具体的で動的な現実に根ざすものであることを示唆しています。この変革は、データの価値と使用方法を変え、文明の未来に影響を与えます。最も重要なことは、IoTeX が実現するすべてのものが人々によって所有され、人々のために運用されることです。

IoTeX コミュニティの皆様の継続的な貢献、サポート、フィードバックに感謝します。この新しい野心的な旅に乗り出すにあたり、IoTeX と私たちのグローバル コミュニティが真の変化をもたらし、DePIN を世界中のすべての国にもたらすと確信しています。構築する時が来ました!

免責事項

このホワイトペーパーは、IoTeX coredev と IoTeX コミュニティのメンバーによる共同作業です。IoTeX ネットワークの提案された方向性を概説しています。ただし、内容は著者またはそれぞれの組織によるコミットメントを伴うものではありません。IoTeX コミュニティは、このホワイトペーパーで提案された対策を適応および採用する責任があります。提案の成功は、最終的には、より広範なコミュニティと IoTeX ネットワーク内で構築する人々の努力にかかるています。

ここで提供される情報は、信頼できる情報に基づいて誠意を持って提供されていますが、正確性や完全性は保証されません。この文書の情報は、投資アドバイス、財務アドバイス、取引アドバイス、またはその他の形式のアドバイスとしてみなされるべきではありません。いかなる種類の投資決定を行う前に、独自のデューデリジェンスを実施し、財務アドバイザーに相談することをお勧めします。

了承

私たちは以下の個人およびベンチャーキャピタル企業に心からの感謝の意を表します(例: Escape Velocity (EV3) の Vinayak Kurap、1kx の Robert Koschig、SNZ Capital、Future Money Group (FMG)、Borderless Capital の Álvaro Gracia、Lattice、Summer Capital、Pantera Capital、BlueYard Capital、Spartan Capital、Lemniscap、NGC Ventures、Stanford Blockchain Accelerator、Foresight Venture、Samsung NEXT)、Web3 プロジェクト(つまり、NEAR Foundation、RISC0、Helium Foundation、The Graph Foundation、Filecoin Foundation)、テキスタイル)、暗号通貨調査会社(IntoTheBlock (ITB) および Messari など)の貴重なフィードバックと揺るぎないサポートが、このホワイトペーパーの作成に役立っています。皆様の専門知識、見識、取り組みにより、私たちの仕事の深みと質が大幅に向上しました。私たちは、皆様が投資してくださった時間とリソースに深く感謝しており、皆様の貢献は IoTeX 2.0 のミッションを前進させる上で極めて重要です。

文献

- [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.