

IoTeX 2.0 – DePIN untuk Semua Orang!

Versi 1.1

The IoTeX Team

17 July 2024

Abstrak

Jaringan infrastruktur fisik terdesentralisasi (DePIN) saat ini menjadi salah satu narasi terpanas di Web3 dan mewakili perubahan paradigma besar yang secara mendasar dapat mengubah cara jaringan infrastruktur fisik dibangun, dioperasikan, dan dikelola dalam waktu dekat. Karena kurangnya dana dan kompetensi teknis, startup DePIN yang baru muncul menghadapi tantangan besar untuk menyampaikan ide mereka ke pasar pada waktu yang tepat. Dalam whitepaper ini, kami menyajikan IoTeX 2.0, sebuah langkah transformatif dalam evolusi jaringan IoTeX, yang bertujuan untuk mengatasi tantangan-tantangan yang disebutkan di atas dan membantu komunitas DePIN mewujudkan visi utama "DePIN untuk Semua Orang!".

IoTeX 2.0 berisi inovasi inti berikut:

- Desain tokennomic baru yang mengeksplorasi kegunaan token IOTX di infrastruktur DePIN modular secara ekstensif;
- Infrastruktur DePIN modular yang memungkinkan startup DePIN membangun aplikasi mereka di atas infrastruktur terdesentralisasi milik komunitas;
- Kumpulan keamanan modular (Modular Security Pool - MSP) yang menyediakan lapisan tepercaya terpadu Modul infrastruktur DePIN melalui penyetelan ulang;
- Jaringan multi-prover terdesentralisasi yang disebut W3bstream yang memungkinkan pembuat DePIN xmemanfaatkan pendekatan bukti validitas yang berbeda untuk mewujudkan verifikasi DePIN;
- Sistem identitas terpadu yang disebut ioID yang mengelola dan mengamankan hubungan mesin-ke-mesin dan mesin-ke-orang secara on-chain/off-chain dalam aplikasi DePIN;
- SDK tertanam universal yang disebut ioConnect yang memberdayakan abstraksi perangkat dan memfasilitasi interaksi perangkat pintar dalam aplikasi DePIN;

- SDK rantai yang disebut ioDDK yang memungkinkan proyek DePIN menyediakan rantai aplikasi yang berdaulat sendiri dan mewarisi keamanan IoTeX L1 secara bersamaan.

Banyak

Bab 1 DePIN Hari Ini	6
1.1 Mengapa DePIN Penting	8
1.2 Lanskap DePIN	9
1.3 Tumpukan Teknologi DePIN dan Tantangannya	10
1.4 Filosofi Kami untuk DePIN	14
Bab 2 IoTeX 2.0	16
2.1 Pendahuluan	16
2.2 Apa yang (Tidak) Kami Bangun	18
2.3 Tokenomics	22
2.3.1 Utilitas IOTX di IoTeX 2.0	23
2.3.2 Imbalan Staking Inflasi	27
2.3.3 Pembakaran Deflasi	28
2.3.4 Insertif Pertumbuhan	30
2.4 Barang Publik	31
2.5 Mendukung Pembangun Sepanjang Siklus Hidup Proyek	34
2.6 Masa Depan	35
Bagian 3 Modular Security Pool (MSP) - Lapisan Tepercaya Terpadu untuk Modul Infrastruktur DePIN	37
3.1 Masalahnya	37
3.2 Pasar Terbuka untuk Keamanan dan Kepercayaan	38
3.3 Arsitektur	39
Bab 4 W3bstream - Jaringan Multi-Prover Terdesentralisasi untuk Verifikasi DePIN	42
4.1 Arsitektur W3bstream	42
4.1.1 Empat Jenis Provers	43
4.1.2 Inovasi In-house Kami pada ZKP	47
4.2 Alur Kerja W3bstream	48
4.2.1 Orientasi dan Manajemen Prover	48
4.2.2 Alur Kerja	48
4.3 Verifikasi DePIN dan AI Off-Chain	49
4.3.1 Verifikasi DePIN	50
4.3.2 AI Luar Rantai	50
Bab 5 ioID - Sistem Identitas Terpadu untuk DePIN	52
5.1 Identitas On-Chain vs. Off-Chain	52
5.1.1 Identitas Dalam Rantai	52
5.1.2 Identitas Luar Rantai	53

5.2 Desain ioID	53
5.2.1 Pembuatan ioID pada Perangkat	54
5.2.2 Pembuatan ioID pada Perangkat	55
5.2.3 Mengamankan Interaksi Mesin-ke-Mesin	57
5.3 Integrasi ioID dalam Proyek DePIN	57
5.3.1 Kontrak Cerdas di ioID	57
5.3.2 Menyebarluaskan Kontrak NFT Perangkat	58
5.3.3 Mendaftarkan Proyek DePIN	58
5.3.4 Mengatur Kontrak NFT Perangkat	59
5.3.5 Meminta ioID	59
5.3.6 Mendaftarkan Perangkat	59
Bab 6 ioConnect - SDK Tertanam Universal untuk Memberdayakan Abstraksi Perangkat	60
6.1 Pilihan Konektivitas	61
6.1.1 Menghubungkan ke Lapisan Konektivitas Terpusat	61
6.1.2 Menghubungkan ke Lapisan Konektivitas Terdesentralisasi	62
6.2 Pertimbangan Desain untuk Membangun SDK Tertanam Universal untuk Perangkat DePIN	63
6.2.1 API Kripto Bersertifikat PSA Arm	63
6.2.2 Identitas Kedaulatan Diri (SSI)	64
6.3 Spesifikasi Implementasi	65
6.3.1 Inti SDK ioConnect	65
6.3.2 Kompatibilitas Perangkat DePIN	66
Bab 7 ioDDK - Mengaktifkan Rantai Aplikasi DePIN yang Berdaulat Sendiri	68
7.1 Alasan Desain	68
7.2 Blockspace dan Validator Bersama	69
7.3 Komponen ioDDK dan Alur Kerja Tingkat Tinggi	72
7.3.1 Komponen ioDDK	72
7.3.2 Alur Kerja Tingkat Tinggi	72
7.4 Pasar Penyewaan Blockspace	73
7.5 Implikasi pada IoTeX L1	73
Bab 8 Peta Jalan Baru	76
Bab 9 Kesimpulan	78

Bab 1

DePIN Hari Ini

IoTeX didirikan pada tahun 2017 untuk memberdayakan masyarakat agar memiliki dan mengendalikan perangkat pintar mereka, serta data dan nilai yang dihasilkan perangkat mereka, dengan menghubungkan Internet of Things (IoT) dengan blockchain. Tesis awal kami adalah bahwa pengaturan miliaran perangkat pintar menggunakan blockchain yang terdesentralisasi akan menyelesaikan permasalahan besar pada Internet of Things yang ada, seperti kepercayaan, keamanan, dan interoperabilitas, serta memungkinkan paradigma baru untuk jaringan perangkat milik pengguna berkembang. Selama 6 tahun terakhir, kami telah memelopori sintesis dunia nyata dan blockchain, mengeksplorasi dan membangun beberapa kasus penggunaan inti:

- **Pembayaran mikro (2017-2018):** Gunakan blockchain sebagai lapisan penyelesaian digital global untuk memfasilitasi pembayaran otomatis dan murah antar perangkat, mesin, dan manusia. Blockchain berfungsi sebagai lapisan pemersatu bagi perangkat yang sebelumnya tidak dapat dioperasikan untuk berkomunikasi dan bertransaksi.
- **Asal dan rantai pasok (2018-2020):** Memanfaatkan blockchain sebagai buku akuntansi dan kepemilikan yang tidak dapat dipercaya, sehingga memungkinkan asal untuk perangkat pintar dan kasus penggunaan rantai pasokan yang terdesentralisasi (misalnya, Pebble Tracker [1,2]). Block-chain mengumpulkan data dari perangkat tepercaya untuk memverifikasi aktivitas dunia nyata serta memicu peristiwa dan alur kerja baru.
- **Kepemilikan dan privasi data (2020-2021):** Gunakan blockchain sebagai lapisan identitas terdesentralisasi untuk memungkinkan orang memiliki dan mengontrol perangkat dan data mereka (misalnya, Ucam [3, 6]), yang menggabungkan kriptografi tingkat lanjut seperti end-to Enkripsi -end, komputasi multi-pihak, dan komputasi rahasia. Solusi privasi terdesentralisasi dikembangkan melalui kemitraan dengan perusahaan besar seperti Arm [7, 8].

- **DePIN (2021-sekarang):** Gunakan blockchain sebagai fondasi **Decentralized Physical Infrastructure Networks** (DePIN), sebuah model baru untuk pembentukan modal dan koordinasi manusia yang memungkinkan masyarakat berkontribusi dan membangun ekuitas dalam jaringan infrastruktur dunia nyata. Data dan layanan yang dihasilkan De-PIN juga dapat berfungsi sebagai masukan untuk kategori kasus penggunaan lainnya, yaitu Kecerdasan Buatan (Artificial Intelligence - AI) dan Aset Dunia Nyata (Real World Assets - RWA).

Whitepaper IoTeX asli [5] yang diterbitkan pada tahun 2017 menunjukkan visi kami untuk L1 yang aman, terukur, multiguna, dan terdesentralisasi yang menggabungkan teknologi menjaga privasi dan middleware berorientasi perangkat untuk menghubungkan dunia fisik dan digital. Selama bertahun-tahun, kami telah mewujudkan banyak tujuan ambisius yang ingin kami capai dalam whitepaper asli kami:

- Mainnet IoTeX telah memproses ~120 juta transaksi tanpa segala waktu henti atau peretasan;
- Perangkat keras pertama yang kompatibel dengan blockchain (misalnya, Ucam dan Pebble Tracker) dirancang dan diproduksi oleh IoTeX sebagai perangkat pengembang perangkat keras yang siap pakai untuk membuat;
- Berbagai perangkat pintar dari pihak ketiga telah terintegrasi ke dalam Platform IoTeX, memberikan pemahaman mendasar tentang cara terhubung dunia nyata dengan aman ke blockchain;
- Seluruh ekosistem proyek DePIN telah diluncurkan di IoTeX menggabungkan data dunia nyata dari perangkat pintar;
- Komunitas global validator jaringan, pengembang, dan pengguna telah bergabung dibuat yang mewakili sumber kehidupan Jaringan IoTeX.

Tapi ini baru permulaan. Lanskap blockchain telah berkembang secara eksponensial sejak tahun 2017 dan kami sekarang memiliki pemahaman yang lebih mendalam tentang apa yang diperlukan De-PIN untuk mencapai adopsi massal. Sejalan dengan membangun visi IoTeX asli kami, coredev IoTeX sibuk meneliti dan merancang inovasi baru untuk membawa DePIN ke tingkat berikutnya, seperti bukti tanpa pengetahuan, penskalaan off-chain, identitas kedaulatan mandiri untuk perangkat, dan barang publik.

yang mendorong kemajuan seluruh sektor DePIN. Visi IoTeX 2.0 yang kami perkenalkan menguraikan rencana tiga tahun kami untuk memperluas Jaringan IoTeX. Kami bertujuan untuk menggabungkan desain platform modular baru, memperbarui tokennomics kami, dan banyak lagi untuk memenuhi permintaan yang semakin meningkat dari para pembangun di bidang DePIN dan seterusnya. Dengan visi yang diperbarui

ini, kami akhirnya dapat mewujudkan tujuan utama kami dalam memberdayakan "**DePIN untuk Semua Orang!**".

1.1 Mengapa DePIN Penting

Sebelum kita mendalami IoTeX 2.0 dan visi kami untuk masa depan DePIN, kami ingin memulai dengan berbagi apa itu DePIN dan mengapa Anda harus peduli. Saat ini, banyak industri dan utilitas publik terpenting di dunia, seperti telekomunikasi, energi, dan komputasi, merupakan monopoli dan oligopoli yang dimiliki dan dikendalikan oleh perusahaan dan pemerintah yang tersentralisasi. Industri bernilai triliunan dolar ini dirancang dengan hambatan masuk yang sangat tinggi, baik finansial maupun logistik; misalnya, AT&T menghabiskan \$24 miliar per tahun dan membutuhkan lebih dari 160.000 karyawan untuk menjalankan kerajaan telekomunikasi mereka. Karena besarnya hambatan masuk ini, hanya ada sedikit penyedia barang dan jasa yang dapat dipilih oleh masyarakat umum. Hal ini berarti persaingan menjadi terbatas, inovasi terhambat, dan konsumen harus menerima layanan pelanggan yang di bawah standar dan harga yang terlalu melambung karena mereka tidak mempunyai pilihan lain. Saat mereka memberikan layanan kepada jutaan pelanggan, perusahaan raksasa juga secara diam-diam mengekstrak data sensitif dan berharga dari masyarakat demi keuntungan mereka sendiri. Permasalahan yang diakibatkan oleh hal ini bahkan lebih parah lagi terjadi di negara-negara emerging market, yang semakin memperdalam kesenjangan kekayaan dan membatasi peluang bagi masyarakat umum.

DePIN adalah konsep revolusioner yang akan mengubah status quo. DePIN yang dibangun di atas blockchain sumber terbuka dan terdesentralisasi dapat menghadirkan transparansi, kepercayaan, dan inovasi pada infrastruktur fisik dan utilitas publik yang melayani miliaran orang di seluruh dunia dengan biaya rendah atau tanpa biaya. Namun memperbaiki dunia saat ini hanyalah sebagian kecil dari potensi DePIN yang sebenarnya. Peluang sebenarnya bukan sekedar memperbaiki apa yang salah dengan dunia saat ini,

namun membangun dunia baru dengan utilitas yang dimiliki, dioperasikan, dan dimanfaatkan oleh masyarakat sehari-hari. DePIN akan memungkinkan siapa pun untuk berkontribusi dan membangun ekuitas dalam jaringan infrastruktur dunia nyata, mengatasi hambatan masuk finansial dan logistik yang disebutkan di atas. Dengan memanfaatkan metode pembentukan modal baru yang dipopulerkan oleh Decentralized Finance (DeFi) untuk mengumpulkan sumber daya jaringan, DePIN dapat mengumpulkan perangkat keras, tenaga kerja, dan keahlian regional yang dikontribusikan pengguna untuk mendorong pembangunan jaringan infrastruktur baru dan memberikan penghargaan kepada kontributor dengan ekuitas dalam jaringan yang mereka bantu ciptakan. Terakhir, DePIN dapat memanfaatkan kontrak pintar yang tidak dapat diubah di blockchain untuk memverifikasi dan mengoordinasikan tindakan kontributor demi memberikan yang terbaik bagi jaringan.

DePIN tidak hanya memberikan jalan untuk memperbaiki dunia kita saat ini, namun juga menawarkan kesempatan untuk merancang dunia yang lebih baik. Kita berada di ambang revolusi industri baru di mana infrastruktur yang sudah berumur puluhan tahun, seperti bahan bakar fosil dan internet kabel, akan digantikan oleh infrastruktur inovatif, seperti energi terbarukan dan nirkabel. Dengan DePIN, setiap orang dapat menjadi kontributor modernisasi infrastruktur global dan menerima bagian yang adil dari nilai triliunan dolar yang diwakili oleh infrastruktur ini. Dunia baru oleh masyarakat, untuk masyarakat – itulah janji DePIN. DePIN, untuk semua orang!

1.2 Lanskap DePIN

DePIN adalah upaya kolektif dari ratusan proyek di seluruh dunia yang semuanya mengarah pada desentralisasi dan peningkatan infrastruktur fisik kita. Meskipun istilah DePIN diciptakan pada tahun 2023, sektor DePIN telah aktif lebih lama dengan proyek-proyek seperti IoTeX, Helium, dan Filecoin yang menjadi pionir sejak tahun 2017. Saat ini, lanskap DePIN beragam dan terdiri dari proyek-proyek yang membangun khusus DePIN. infrastruktur serta aplikasi DePIN di beberapa vertikal. DePIN kini menjadi salah satu kasus penggunaan blockchain yang paling menjanjikan dan dapat dibagi lagi menjadi jaringan sumber daya fisik dan jaringan sumber daya digital, yang ditentukan berdasarkan jenis layanan yang disediakan jaringan. Jaringan sumber daya fisik menghasilkan sumber daya yang tidak dapat dipertukarkan (yaitu, data/layanan dari perangkat apa pun bersifat unik) yang sifatnya lebih nyata dan umumnya

bergantung pada perangkat keras yang bergantung pada lokasi. Di sisi lain, jaringan sumber daya digital menghasilkan pasar untuk sumber daya yang dapat dipertukarkan (yaitu, penyimpanan 1 GB berarti penyimpanan 1 GB) yang lebih bersifat virtual dan bergantung pada perangkat keras yang tidak bergantung pada lokasi. Sektor DePIN juga mencakup infrastruktur dan peralatan yang memfasilitasi pertumbuhan kategori ini dan menyediakan kemampuan siap pakai untuk aplikasi DePIN. Lanskap DePIN yang komprehensif ditunjukkan pada Gambar 1.1.

1.3 Tumpukan Teknologi DePIN dan Tantangannya

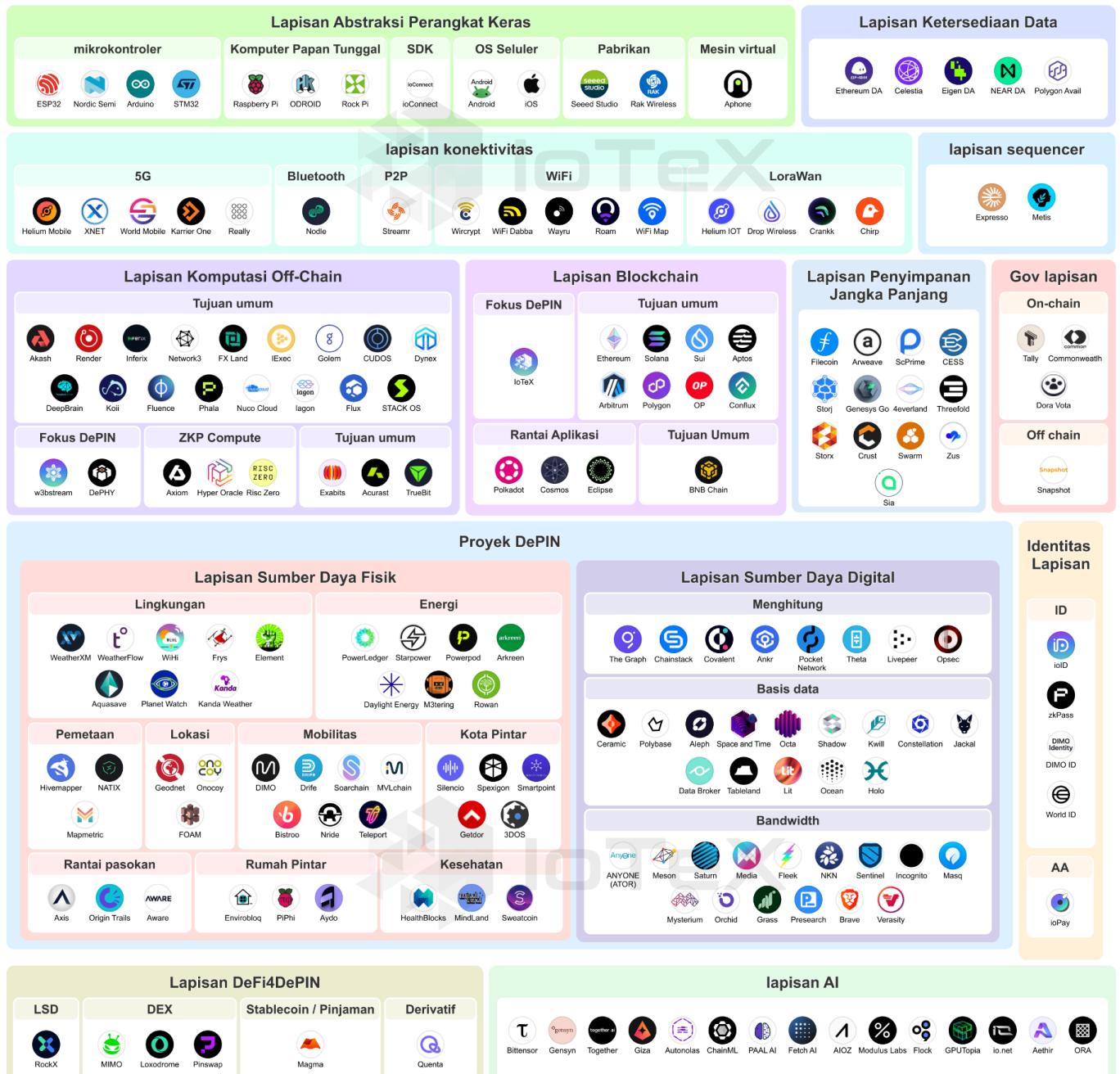
Terlepas dari apakah DePIN berfokus pada sumber daya fisik atau sumber daya digital, atau vertikal spesifik apa yang mereka targetkan, kebutuhan akan tumpukan teknologi end-to-end yang menghubungkan dunia nyata ke dunia blockchain sangatlah penting. Tidak seperti kasus penggunaan blockchain yang memfasilitasi pertukaran aset digital seperti NFT dan aset keuangan seperti stablecoin, DePIN harus berinteraksi dengan perangkat pintar dunia nyata yang menghasilkan data dalam jumlah luar biasa. Blockchain, sebagai buku besar yang tidak dapat diubah, adalah landasan sempurna untuk mendokumentasikan fakta tentang apa yang terjadi di dunia nyata; namun, sebelum menulis "bukti aktivitas dunia nyata" dari perangkat ke blockchain secara permanen, serangkaian langkah harus diselesaikan untuk memverifikasi aktivitas dunia nyata yang benar-benar terjadi dan datanya dapat dipercaya. Perangkat harus didaftarkan secara on-chain, data mentah harus dikumpulkan, diurai, dan disimpan, dan komputasi atas data harus dilakukan dengan cara yang dapat diverifikasi sebelum "bukti aktivitas dunia nyata" dapat diselesaikan ke dalam blockchain. Arsitektur referensi [9]



DePIN Lanskap

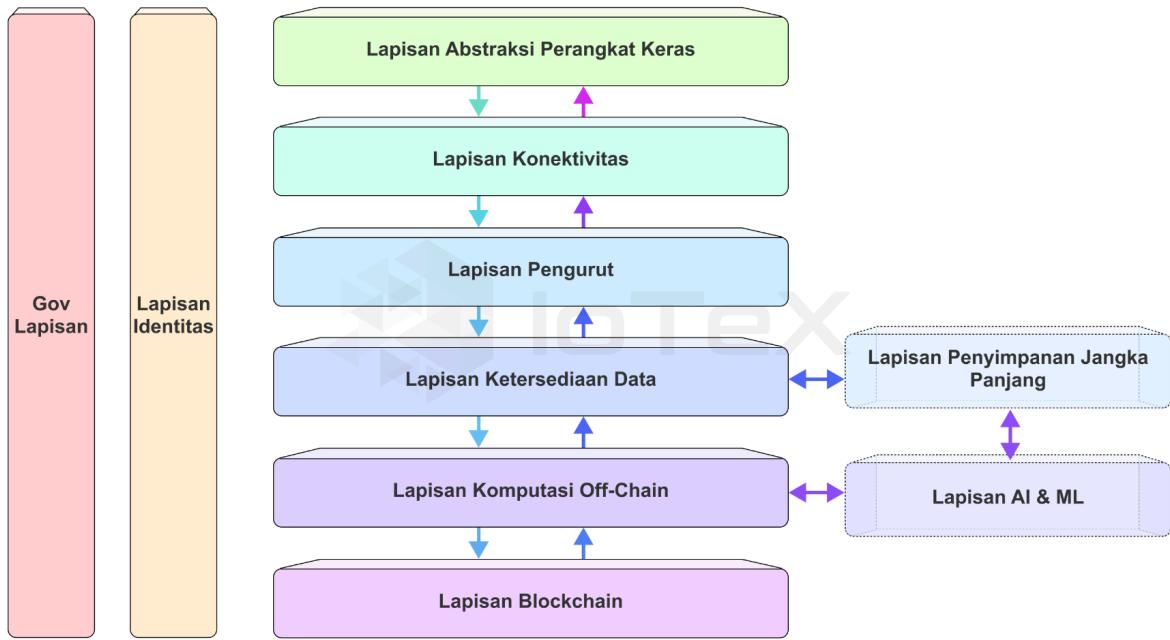
JUL 2024

Jaringan Infrastruktur Fisik Yang Terdesentralisasi



Gambar 1.1: Lanskap DePIN

seperti yang ditunjukkan pada Gambar 1.2 memperkenalkan sembilan lapisan penting yang perlu dipertimbangkan oleh proyek DePIN.



Gambar 1.2: Tumpukan Teknologi DePIN

- **Lapisan Abstraksi Perangkat Keras**: memfasilitasi berbagai perangkat pintar, besar atau kecil, untuk terhubung secara aman dengan entitas di Lapisan Konektivitas
- **Lapisan Konektivitas**: menyampaikan data yang dihasilkan oleh perangkat pintar secara andal ke Lapisan Pengurut
- **Lapisan Sequencer**: memesan paket data dari perangkat pintar sebelum mengirimkannya ke Lapisan Ketersediaan Data
- **Lapisan Ketersediaan Data**: menyimpan data untuk penggunaan segera dan verifikasi keamanan, memungkinkan perangkat off-chain mengakses informasi dan menghasilkan wawasan dari data mentah
- **Lapisan Penyimpanan Jangka Panjang**: mengarsipkan data mentah dan wawasan untuk penggunaan di masa mendatang, yang dapat diakses oleh pihak ketiga melalui API untuk kepatuhan, analisis, AI, dan banyak lagi
- **Lapisan Komputasi Off-Chain**: menerapkan logika bisnis pada data yang disimpan di Lapisan Ketersediaan Data untuk menghasilkan wawasan dan bukti terkait aktivitas dunia nyata

- **Lapisan Blockchain:** berfungsi sebagai jangkar kepercayaan untuk identitas dan data perangkat, memverifikasi validitas perhitungan off-chain dan mendistribusikan hadiah token kepada pemangku kepentingan DePIN
- **Lapisan Identitas:** mengelola identitas on-chain dan/atau off-chain untuk semua entitas yang terlibat (misalnya, perangkat pintar, pengguna, server, produsen, validator)
- **Lapisan Tata Kelola:** menegakkan kebijakan dan prosedur jaringan (misalnya, insentif) dengan cara yang terdesentralisasi, biasanya melalui proses pemungutan suara komunitas.

Lapisan tumpukan teknologi DePIN yang luas bisa sangat melelahkan bagi satu tim untuk berkembang secara monolitik. Kompleksitas ini menciptakan hambatan besar bagi para pembangun untuk bereksperimen dengan ide-ide inovatif di DePIN. Dalam beberapa tahun terakhir, proyek-proyek yang didanai dengan baik telah mengatasi tantangan-tantangan ini dengan meningkatkan modal ventura secara signifikan dan mengembangkan teknologi monolitik mereka sendiri. Namun, agar DePIN benar-benar berkembang dan menjangkau seluruh penjuru dunia (seperti LATAM, Afrika, dan Asia Tenggara), banyaknya teknologi dan kompleksitas teknologi yang tinggi menghadirkan tantangan tambahan:

- **Kecepatan Peluncuran:** kecepatan DePIN mencapai ambang batas pasokan minimum untuk mendorong permintaan awal terbatas karena kendala perangkat keras dan persyaratan belanja modal di muka;
- **Pertumbuhan Sisi Permintaan:** DePIN kesulitan dalam meningkatkan permintaan karena perjalanan panjang untuk melakukan bootstrap pasokan dan kesulitan dalam mencapai keseimbangan dengan solusi yang ada dalam hal pengalaman pengguna, keandalan, dan biaya;
- **Likuiditas Token:** DePIN menggunakan insentif token untuk mendorong pertumbuhan jaringan dan mendanai operasi infrastruktur, namun kesulitan dalam menutup roda gila dan membangun likuiditas on-chain;

- **Kesadaran:** DePIN sering kali berfokus pada industri tertentu, dimana tujuan dan ukuran keberhasilan proyek tidak selalu jelas, terutama bagi industri yang belum terlibat langsung dalam industri tersebut.

Karena tantangan ini, DePIN masih terbilang baru dan belum melampaui DeFi dan sektor kripto lainnya dalam hal nilai pasar dan adopsi. DeFi dan DePIN serupa dalam banyak hal, terutama karena keduanya melakukan crowdsourcing sumber daya dari masyarakat (“sisi pasokan”) untuk menciptakan produk yang diinginkan dan digunakan orang lain (“sisi permintaan”). Namun, jalur untuk memperoleh dan mempertahankan pasokan dan permintaan sangat berbeda antara DeFi dan DePIN. Pada tingkat tinggi, pasokan dan permintaan DeFi lebih mudah untuk di-bootstrap tetapi cepat berlalu, sementara pasokan dan permintaan DePIN lebih sulit untuk di-bootstrap tetapi lebih mampu bertahan dalam ujian waktu. Selain itu, DePIN sering kali harus mengumpulkan pasokan sumber daya dalam jumlah besar untuk menciptakan permintaan awal, tidak seperti DeFi di mana sejumlah kecil dana gabungan mungkin memiliki permintaan segera. Membandingkan DePIN dan DeFi secara berdampingan dengan tantangan yang disebutkan di atas, kita dapat melihat perbedaan rinci berikut seperti yang ditunjukkan pada Gambar 1.3.

1.4 Filosofi Kami untuk DePIN

Kami sangat yakin bahwa DePIN diperuntukkan bagi semua orang: setiap pembuat, setiap kontributor, dan setiap pengguna. Keyakinan ini menggarisbawahi bahwa:

- Tim kecil dan bahkan pengembang tunggal harus mampu membangun produk DePIN yang berdampak menggunakan infrastruktur terbaik di kelasnya.
- Proyek DePIN harus diulang dengan cepat tanpa biaya awal yang tinggi untuk mengidentifikasi inovasi nyata.

- Proyek di bawah DePIN harus dapat disusun baik dari segi fungsinya (misalnya, menggabungkan data dari dering, mobil, telepon untuk individu) dan wilayah (seperti model kota-demi-kota Uber).
- Kontributor jaringan yang memberikan nilai atau utilitas pada jaringan harus memiliki persyaratan masuk yang rendah, dan mendapatkan imbalan finansial dalam bentuk yang stabil dan berjangka panjang.
- Pengguna harus dapat menikmati akses yang adil terhadap utilitas publik yang inovatif dari jaringan DePIN ini.

Keyakinan ini bukan sekedar angan-angan belaka. Secara praktis dapat diterjemahkan ke dalam desain teknis, yang dikenal sebagai IoTeX 2.0, seperti yang ditunjukkan di bawah ini.

	DeFi	DePIN	Tantangan untuk DePIN	Solusi Parsial
Tumpukan Teknologi	Sederhana dan hanya digital: misalnya Solidity + JS, mudah untuk diluncurkan	Rumit dan menyentuh dunia fisik: C/C++ + Golang/Python/Rust + Solidity + JS + opsional Swift, sulit untuk bercabang.	Tantangan 1: Proyek DePIN lebih sulit untuk dibangun dan memerlukan lebih banyak modal untuk diluncurkan karena komponen perangkat kerasnya. Eksplorasi lambat dan mahal.	<ul style="list-style-type: none"> • Luncurkan proyek secara terpusat untuk "menguji" pasar dan mempercepat pengambilan keputusan • Kurangnya desentralisasi dan ketidakpercayaan dapat menghalangi kontributor dan investor
Kecepatan Luncurkan	Cepat: misalnya meluncurkan dApp secara global; beberapa "penambang" dengan modal besar mengatur sisi pasokan dengan cepat	Lambat: misalnya mengirimkan dan menerapkan perangkat keras khusus proyek, skala ambang batas pasokan di mana jaringan dapat melayani permintaan mungkin tinggi	Tantangan 2: Proyek DePIN lambat diluncurkan (menetapkan sisi pasokan) karena kendala perangkat kerasnya, yang dapat menyebabkan ketidaksesuaian dengan siklus kripto.	<ul style="list-style-type: none"> • Bekerja sama dengan mitra Web2 yang sudah ada, misalnya T-Mobile, untuk mencapai skala ambang batas dengan lebih cepat • Tidak berlaku untuk jaringan DePIN inovatif yang tidak memiliki mitra Web2
Pertumbuhan Sisi Permintaan	Mudah untuk menarik pengguna jika dirancang dengan benar, misalnya pertanian hasil panen, tetapi biasanya berumur pendek	Lambat dalam melakukan bootstrap, misalnya dalam menerima pelanggan paket seluler, namun bisa lebih berdampak dalam jangka panjang	Tantangan 3: Kripto dapat memberikan UX yang rumit dan tidak diperlukan, sehingga memperlambat adopsi sisi permintaan	<ul style="list-style-type: none"> • Menggunakan token untuk memberi insentif kepada masyarakat umum agar mengadopsi dan menggunakan DePIN • Kebanyakan orang bukan asli kripto dan tidak memahami token, wallet, dll.
Likuiditas token	Token liquidity is easy to acquire and a natural byproduct of a financial application	Likuiditas token seringkali sulit dicapai karena pendiri dan kontributor memiliki lebih banyak pengalaman perangkat keras dan Web2 daripada pengalaman finansial	Tantangan 4: Likuiditas token penting untuk proyek kripto apa pun, terutama untuk DePIN yang mendorong pertumbuhan jaringan dengan insentif token	<ul style="list-style-type: none"> • Tim DePIN dapat bekerja dengan CEX dan pembuat pasar untuk mendapatkan likuiditas token • Ini bisa menjadi proses yang mahal dan memakan waktu
Berbagi pertumbuhan jaringan	Metric kesuksesannya jelas, misalnya TVL dan mudah ditarik serta ditampilkan	Metric keberhasilan bersifat spesifik proyek dan harus diambil dari perangkat fisik	Tantangan 5: Tim DePIN harus menghabiskan waktu dan upaya yang berharga untuk membangun dasbor untuk menampilkan metrik proyek mereka	<ul style="list-style-type: none"> • Data on-chain dapat dengan mudah ditarik dan ditampilkan dengan alat seperti Dune • Namun banyak DePIN yang mulai tersentralisasi dan tidak memiliki banyak data on-chain untuk ditampilkan

Gambar 1.3: Perbandingan antara DePIN dan DeFi

Bab 2

IoTeX 2.0

2.1 Pendahuluan

IoTeX 2.0 mendefinisikan visi besar dan peta jalan Jaringan IoTeX untuk beberapa tahun ke depan, memperluas misi kami untuk memungkinkan "DePIN untuk Semua Orang" dan berasal dari pengalaman bertahun-tahun sebagai pionir industri DePIN. Tujuan kami bukan hanya untuk mengatasi tantangan teknis dan non-teknis yang dihadapi proyek DePIN saat ini, namun untuk mewujudkan potensi penuh DePIN di masa depan dengan menjadikan IoTeX ekosistem DePIN terbesar di dunia. Untuk mencapai hal ini, kami sangat bersemangat untuk mempersesembahkan IoTeX 2.0, yang menggabungkan filosofi, teknologi, tokenomics, barang publik, dan inisiatif baru untuk memungkinkan masyarakat berkontribusi pada DePIN dan memberdayakan pembangun untuk benar-benar menjembatani dunia nyata ke dunia blockchain.

Dengan IoTeX 2.0, Jaringan IoTeX akan berkembang dari sekedar blockchain L1 menjadi infrastruktur DePIN terbuka, Dapps, dan L2 yang akan ditambatkan melalui token IOTX. Hal ini akan sangat meningkatkan jumlah dan jenis peserta serta kontributor Jaringan IoTeX yang pada akhirnya memperluas jangkauan IoTeX dan DePIN ke tingkatan baru. DePIN harus diperuntukkan bagi semua orang, itulah sebabnya IoTeX

2.0 memprioritaskan penyertaan pembangun dan pengguna di setiap tahap siklus hidup. Apakah Anda seorang Dapp mapan yang ingin memperluas ke L2 Anda sendiri rantai, atau perusahaan tradisional yang ingin menerapkan model bisnis berbasis DePIN, atau hanya tim kecil dengan ide besar, IoTeX 2.0 menyediakan rangkaian kemampuan lengkap yang relevan untuk semua pembuat DePIN.

Metodologi inti kami adalah infrastruktur DePIN modular: proyek DePIN dapat membangun tumpukan teknologi yang sesuai dengan tahapan dan kebutuhan spesifiknya dengan memilih dari menu penawaran modular. Penawaran ini mencakup produk internal yang dibuat oleh coredev IoTeX dan produk mitra dari proyek-proyek terkemuka. Keuntungan utama dari pendekatan modular adalah memungkinkan pembangun infrastruktur untuk fokus pada fungsi-fungsi yang mereka lakukan dengan

sebaiknya dan berkolaborasi untuk mencapai tujuan bersama. Penawaran modular kami menggabungkan teknologi mutakhir seperti penskalaan off-chain, bukti tanpa pengetahuan, dan kecerdasan buatan untuk menghadirkan inovasi unik ke sektor DePIN. Modul-modul ini dibangun tidak hanya oleh coredev IoTeX tetapi juga oleh pembangun infrastruktur khusus, menggunakan IoTeX untuk memastikan keamanan dan kepercayaannya. Pendekatan ini memberikan solusi komprehensif kepada tim DePIN terbesar, sekaligus menawarkan solusi yang dibuat khusus untuk tim yang lebih kecil yang dapat mereka gunakan untuk membuat proyek DePIN baru dengan cepat dan aman.

Dari perspektif arsitektur, IoTeX 2.0 menekankan perspektif berikut (lihat Gambar 2.1):

- **Kelompok Keamanan Modular (MSP):** Dasar modularitas adalah lapisan terpadu dan tepercaya, yang didukung oleh IOTX dan aset arus utama lainnya, yang kami sebut sebagai MSP. Ini adalah serangkaian kontrak pintar yang diterapkan pada IoTeX L1. Baik IoTeX L1 dan MSP berfungsi sebagai jangkar kepercayaan dan buku besar yang tidak dapat diubah untuk semua aktivitas dalam Lapisan Modul Infrastruktur DePIN (DIM) dan lapisan Dapp/L2. Secara umum, MSP memungkinkan IoTeX L1 untuk meminjamkan keamanan bukti kepemilikannya ke DIM yang menjangkau berbagai bagian tumpukan teknologi DePIN. Penyedia DIM akan mempertaruhkan IOTX dan aset utama lainnya untuk bergabung dengan MSP. Selain itu, DIM yang mendapatkan keamanan dan kepercayaan dari MSP akan secara berkala mengaitkan statusnya ke IoTeX L1, sehingga membuka kemungkinan bagi pembuat dApp untuk berinovasi berdasarkan aktivitas dunia nyata yang tepercaya.
- **Modul Infrastruktur DePIN (DIM):** Lapisan DIM baru di IoTeX 2.0 menawarkan serangkaian fitur modular yang mencakup seluruh tumpukan teknologi DePIN. Sambil mempromosikan kontribusi dari pembangun global, coredev IoTeX akan menyediakan implementasi internal untuk beberapa lapisan. DIM tambahan seperti inferensi AI, penyimpanan, komputasi yang menjaga privasi, analisis data, RPC, dan sistem nama domain akan disediakan oleh mitra dan pembangun yang akan mempertaruhkan IOTX ke MSP. Perhatikan bahwa setiap DIM dapat memiliki tokennya sendiri jika diperlukan.
- **Barang Publik:** Tujuan IoTeX adalah membawa DePIN ke batas baru, yang membutuhkan barang publik yang dapat dipercaya dan digunakan secara bebas

oleh siapa pun. Sasaran kami adalah memimpin gerakan DePIN dengan menciptakan serangkaian sumber daya sumber terbuka yang dapat diintegrasikan dengan mulus oleh para pembuat dan ditawarkan kepada penggunanya untuk mendorong partisipasi terbuka. Barang publik ini mencakup alat yang dapat diakses oleh pengguna (misalnya penjelajah, dompet, jembatan), alat yang berfokus pada pengembang (misalnya IDE), dan sumber daya jaringan (misalnya tata kelola, pendanaan).

- **Tokenomics Meritocratic:** Penambahan lapisan baru pada Jaringan IoTeX menghadirkan pemangku kepentingan baru, yang akan menyumbangkan keahlian di berbagai kategori. Tujuan dari tokennomics kami yang diperbarui bukan hanya untuk memperluas kegunaan token IOTX, namun untuk melakukannya dengan cara meritokratis di mana penghargaan didistribusikan berdasarkan signifikansi kontribusi pemangku kepentingan. Cakupan Jaringan IoTeX yang diperluas akan mendorong utilitas baru pada token IOTX, menjadikannya mata uang dasar sektor DePIN.
- **DePIN Dapps & DePIN L2:** Di puncak teknologi akan terdapat ekosistem DePIN Dapps dan L2 yang memanfaatkan sebagian atau seluruh DIM IoTeX 2.0. Meskipun banyak Dapps yang memilih untuk meluncurkan token asli mereka di IoTeX L1 dan memanfaatkan semua penawaran DIM, beberapa Dapps mungkin hanya memilih untuk menggunakan satu atau lebih DIM. Fokus modular pada IoTeX 2.0 memungkinkan Dapps memanfaatkan berbagai modul berdasarkan kebutuhan kondisi mereka saat ini, sekaligus menyediakan kemampuan baru untuk kebutuhan masa depan mereka. Selain itu, komponen baru dari lapisan DIM adalah ioDDK, sebuah SDK rantai L2 yang memungkinkan proyek meluncurkan L2 mereka sendiri di atas IoTeX L1. Hal ini akan memungkinkan DePIN untuk menciptakan token ekonomi berdaulatnya sendiri dan menghosting Dapps mereka sendiri, sambil memanfaatkan kemampuan luas lapisan DIM serta mendapatkan keamanan dan kepercayaan dari IoTeX L1.

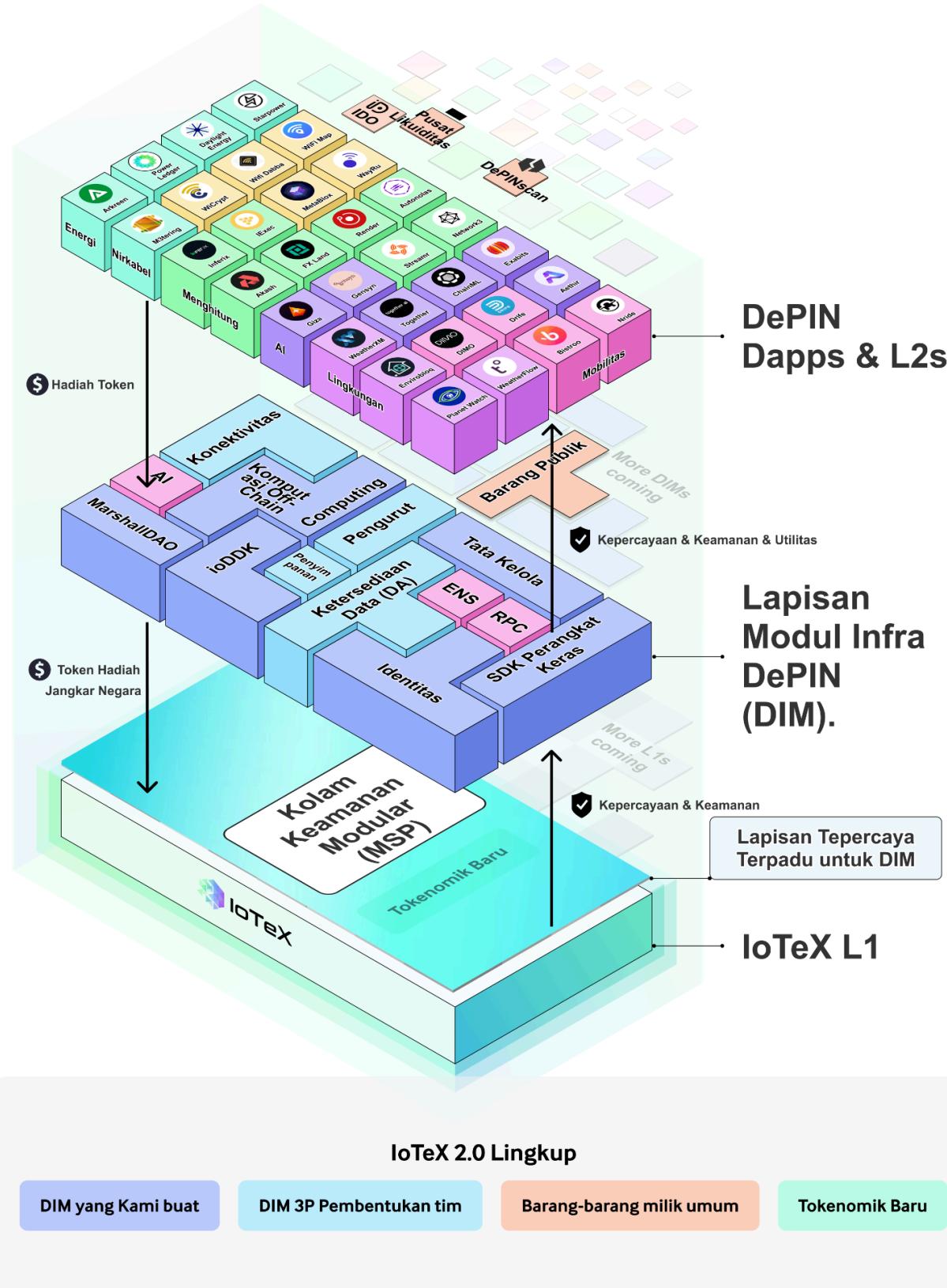
2.2 Apa yang (Tidak) Kami Bangun

Seperti disebutkan dalam Bagian 1.3, membangun DePIN memerlukan tumpukan teknologi berlapis-lapis (lihat Gambar 2.2), yang mencakup berbagai kemampuan. Lapisan DIM IoTeX 2.0 yang baru diperkenalkan menawarkan solusi untuk setiap elemen tumpukan teknologi ini. Lapisan DIM ini sepenuhnya terbuka, memungkinkan setiap pembangun infrastruktur untuk menerapkan implementasinya. Hal ini memberi proyek DePIN beragam pilihan untuk membuat tumpukan teknologi khusus mereka.

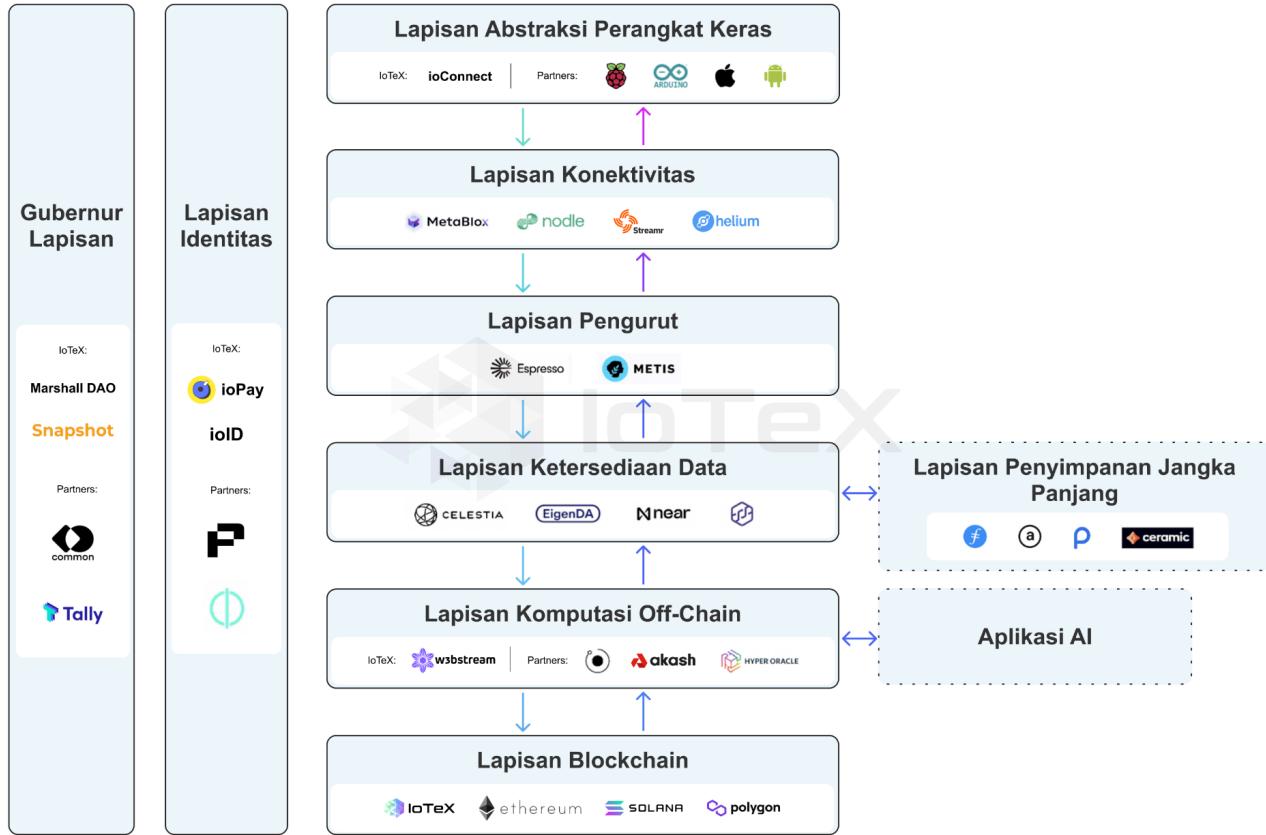
Seiring dengan modul inti yang dikembangkan secara internal oleh coredev IoTeX, banyak modul akan bersumber dari proyek terkemuka di bidang blockchain dengan kemampuan khusus. Misalnya, lapisan Ketersediaan Data adalah fokus utama proyek seperti Celestia dan NEAR, sedangkan lapisan Penyimpanan Jangka Panjang adalah fokus utama proyek seperti Filecoin dan Arweave. Karena IoTeX 2.0 menekankan modularitas dan komposisi, kami mengundang semua proyek untuk berintegrasi ke dalam lapisan DIM, sehingga memungkinkan proyek DePIN merancang tumpukan teknologi pilihan mereka.

Meskipun kami secara terbuka menyambut baik penawaran di bagian mana pun dari lapisan DIM, coredev IoTeX telah meneliti dan mengembangkan solusi canggih untuk beberapa modul penting yang berfokus pada lapisan tepercaya terpadu untuk DIM, perangkat keras, identitas, komputasi off-chain., SDK L2 dan barang publik, yang kami rangkum di bawah dan jelajahi secara mendetail di seluruh bagian berikut.

- **MSP (Lapisan Tepercaya Terpadu untuk DIM):** Ini adalah lapisan tepercaya terpadu yang terdiri dari serangkaian kontrak pintar di IoTeX L1. Dibutuhkan IOTX yang dipertaruhan dan aset utama lainnya dan menyewakan keamanannya ke DIM lain.
- **W3bstream (DIM Komputasi Off-Chain):** Jaringan komputasi off-chain terdesentralisasi pertama di dunia yang memanfaatkan internal dan pihak ketiga



Gambar 2.1: Ruang Lingkup IoTeX 2.0



Gambar 2.2: Modul Infrastruktur DePIN (DIM)

teknologi komputasi yang dapat diverifikasi seperti bukti tanpa pengetahuan (ZKPs), lingkungan eksekusi tepercaya (TEEs), komputasi multi-pihak (MPC), dan enkripsi homomorfik penuh (FHE) untuk vendor yang berbeda untuk menghasilkan "bukti aktivitas dunia nyata" secara nyata. waktu, dan selesaikan bukti-bukti ini ke blockchain untuk memberi penghargaan kepada pemilik perangkat.

- **ioID (Identity DIM):** Rangkaian identitas digital berdaulat mandiri on-chain dan off-chain yang memungkinkan manusia dan mesin membangun hubungan digital yang kaya dan berinteraksi satu sama lain tanpa bergantung pada penyedia identitas terpusat.
- **ioConnect (DIM Abstraksi Perangkat Keras):** SDK yang memungkinkan berbagai perangkat keras terhubung dengan W3bstream dan berbagai L1/L2. Ini berfungsi sebagai lapisan abstraksi perangkat keras yang bekerja dengan lancar pada platform perangkat keras mainstream seperti Raspberry Pi, ESP32, dan Arduino, menyederhanakan kompleksitas penanganan perangkat keras. Dengan kata lain, perangkat yang didukung oleh ioConnect dapat dengan mudah

diintegrasikan ke dalam berbagai aplikasi DePIN, yang berfungsi sebagai multi-penambang.

- **ioDDK (L2 SDK DIM):**SDK rantai yang memungkinkan pembuat DePIN memulai blockchain L2 mereka sendiri dengan lancar sambil menikmati keamanan dari IoTeX L1. Ini secara asli mendukung modul IoTeX seperti W3bstream, ioID, dan De- PINscan.
- SDK rantai yang memungkinkan pembuat DePIN memulai blockchain L2 mereka sendiri dengan lancar sambil menikmati keamanan dari IoTeX L1. Ini secara asli mendukung modul IoTeX seperti W3bstream, ioID, dan De- PINscan. Blockchain IoTeX L1 kompatibel dengan EVM dan menjalankan mekanisme konsensus Roll-DPoS internal kami untuk mencapai 1.000+ TPS. Ruang lingkup dan utilitas IoTeX L1 akan diperluas di IoTeX 2.0: ioID akan diperluas terdaftar ke IoTeX L1, MSP akan diterapkan sebagai kontrak pintar IoTeX L1, dan ioDDK akan mengaitkan rantai L2 ke IoTeX L1.
- Barang Publik: Kami akan terus mengembangkan barang publik yang sudah ada, misalnya seperti DePINScan [23] dan DePIN Liquidity Hub [21], serta build public barang untuk pembuat DePIN.

2.3 Tokenomics

Token IOTX diperkenalkan pada tahun 2019 sebagai mata uang dasar untuk IoTeX L1. Sejak peluncuran Mainnet, token IOTX telah secara efektif menyeimbangkan insentif antara validator (atau “Delegasi”), pembuat Dapp, dan pengguna. Delegasi yang mempertaruhkan IOTX dan memvalidasi transaksi blockchain sebagai bagian dari konsensus jaringan menerima imbalan IOTX, sementara pengembang dan pengguna yang terdiri dari Dapps, pemegang token, dan lainnya membayar IOTX untuk mengirim transaksi dan berinteraksi dengan kontrak pintar. Token IOTX juga dipertaruhkan oleh berbagai jenis pemegang token untuk berpartisipasi dalam tata kelola jaringan secara luas.

Ketika IoTeX berkembang dari sekedar L1 menjadi platform modular infrastruktur yang saling terhubung, tokennomics yang terkait dengan token IOTX juga akan diperluas agar sesuai dengan visi kami untuk IoTeX 2.0. Ini termasuk bentuk utilitas baru untuk token IOTX, yang akan dimasukkan ke dalam penawaran teknologi baru IoTeX

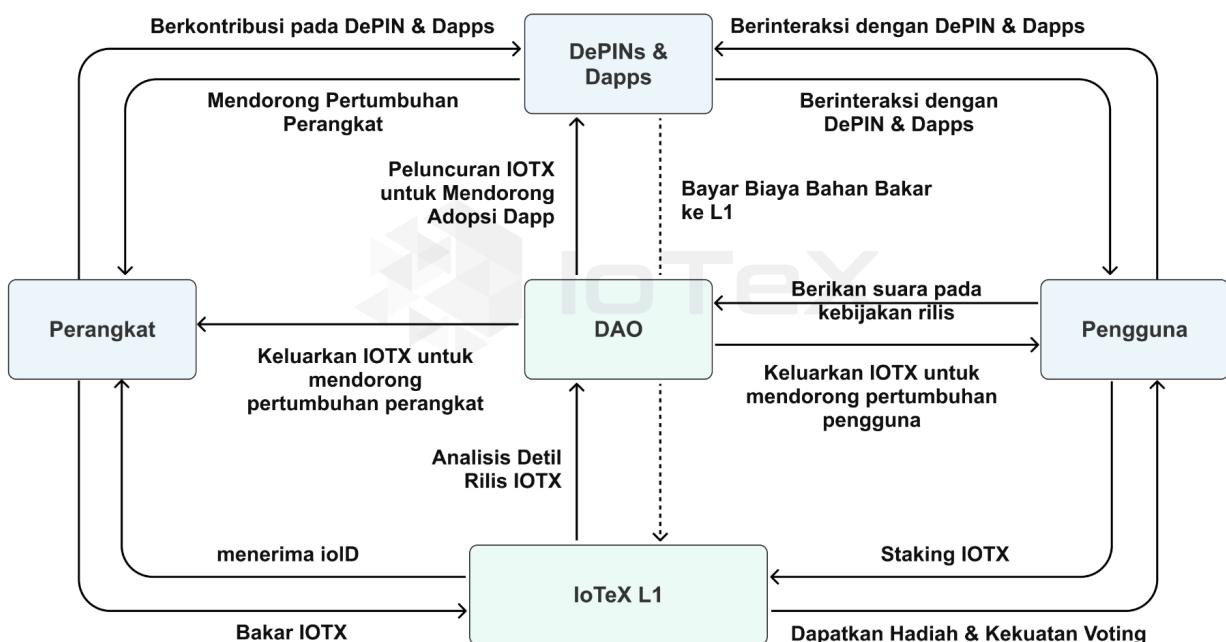
2.0. Selain itu, tujuan penting lainnya dari tokennomics IoTeX 2.0 adalah untuk menyeimbangkan imbalan staking yang bersifat inflasi, pembakaran token yang bersifat deflasi berdasarkan penggunaan platform, dan memberikan insentif kepada DePIN Dapps dan L2 untuk memanfaatkan infrastruktur modular kami. Ini berarti bahwa tokennomics kami yang ditingkatkan tidak hanya akan membawa utilitas dan nilai baru pada token IOTX dengan menghubungkannya ke W3bstream, ioID, ioDDK, dan DIM lainnya, namun juga menjaga pasokan token yang stabil melalui penyeimbangan mekanisme inflasi dan deflasi. Dengan meningkatnya adopsi penawaran infrastruktur modular IoTeX, token IOTX akan memperoleh nilai baru sebagai mata uang jaringan IoTeX 2.0.

2.3.1 Utilitas IOTX di IoTeX 2.0

Token IOTX akan digunakan di seluruh infrastruktur dan ekosistem IoTeX 2.0, dan dapat dilihat dari berbagai perspektif, seperti yang diilustrasikan pada Gambar 2.3 dan 2.4.

- **Dari Perspektif IoTeX L1:** Delegasi akan mempertaruhkan IOTX agar memenuhi syarat untuk memvalidasi transaksi jaringan dan berpartisipasi dalam konsensus, dan akan menerima token IOTX sebagai hadiah atas layanan mereka. Pemegang Token juga dapat mempertaruhkan IOTX untuk memilih Delegasi dan menerima hadiah IOTX. Token IOTX akan terus berfungsi sebagai mata uang asli dari blockchain IoTeX L1 di IoTeX 2.0, di mana Dapps yang ingin menerapkan kontrak pintar dan memproses transaksi pada blockchain IoTeX L1 akan menggunakan IOTX sebagai biaya bahan bakar. Selain mempertaruhkan IOTX untuk berpartisipasi dalam tata kelola, pengguna juga dapat menggunakan IOTX sebagai biaya bahan bakar untuk memproses transaksi di IoTeX L1 dan berinteraksi dengan Dapps dengan menyumbangkan modal dan sumber daya mereka untuk mendapatkan imbalan. Di IoTeX 2.0, pemilik perangkat juga dapat membakar IOTX untuk mendaftarkan perangkat mereka ke IoTeX L1 dan menerima ioID, yang menyediakan jangkar tepercaya untuk partisipasi dalam DePIN. Terakhir, untuk membuat roda gila, IoTeX L1 akan menggunakan DAO di mana pemegang token dapat memilih bagaimana insentif jaringan dialokasikan ke

Roda Gila DePIN



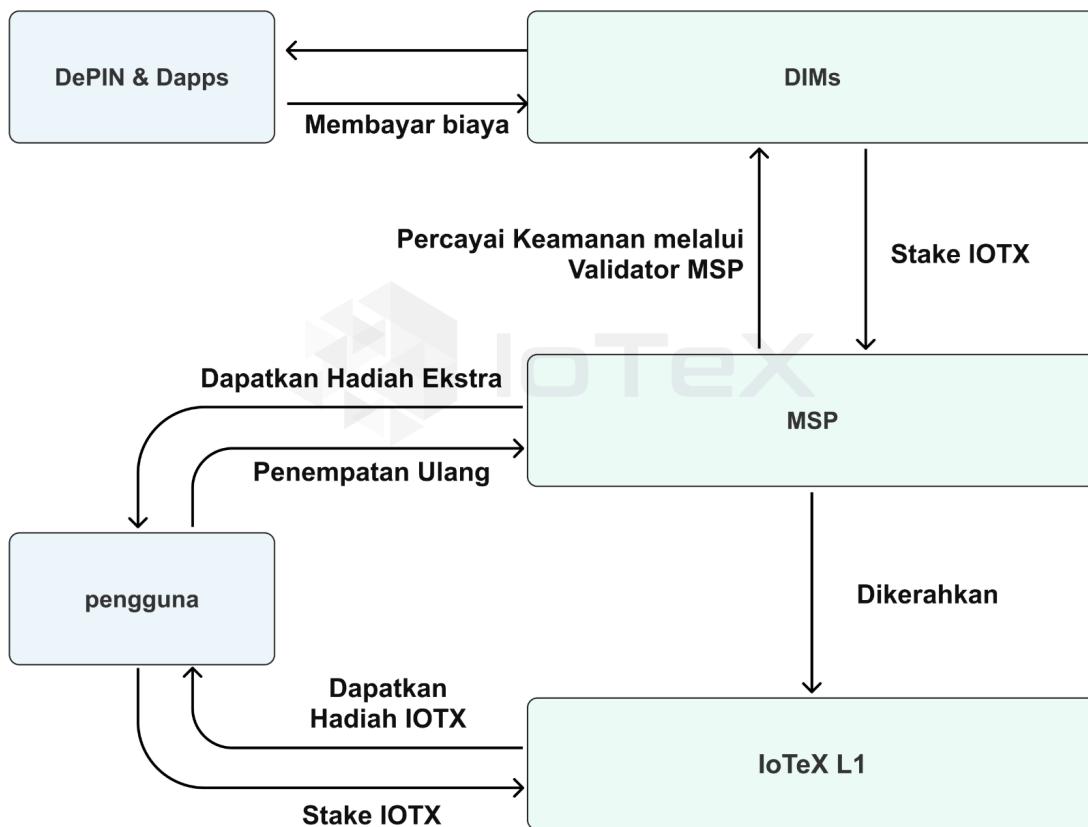
Gambar 2.3: Roda Gila DePIN dan Utilitas Token IOTX

berbagai inisiatif dengan tujuan mendorong perangkat, DePIN, Dapps, dan pengguna baru. Semakin banyak perangkat, DePIN, Dapps, dan pengguna yang terpasang, semakin banyak utilitas IOTX pada IoTeX L1 melalui pembakaran, staking, dan pengeluaran IOTX..

- **Dari Perspektif Modular Security Pool (MSP):** IoTeX 2.0 akan memungkinkan pengguna untuk menggunakan kembali IOTX yang mereka staking dengan melakukan staking ulang atau melakukan hipotesa ulang ke Modular Security Pool (MSP), yang dirancang untuk memperluas keamanan blockchain IoTeX L1 ke DIM yang terintegrasi penawaran mereka ke IoTeX 2.0. Dengan menggunakan MSP, pembuat DIM dapat memberi insentif kepada pemangku kepentingan IOTX untuk mengalokasikan IOTX yang dipertaruhan ulang guna memberikan keamanan pada solusi mereka. Hal ini memperkenalkan ekonomi baru yang menggabungkan IOTX yang dipertaruhan di mana MSP akan secara efektif "menyewakan" keamanan dan kepercayaan kepada DIM, yang akan diperlukan untuk mempertaruhan IOTX. Hal ini juga memungkinkan peluang penghasilan baru bagi

para pemangku kepentingan IOTX, yang akan mendapatkan imbalan staking IOTX dasar yang sama serta imbalan tambahan.

MSP & DIMs



Gambar 2.4: Kegunaan Token IOTX di MSP dan DIM

untuk mempertaruhkan kembali token IOTX yang mereka pertaruhkan, ditambah potensi suap dari proyek DIM.

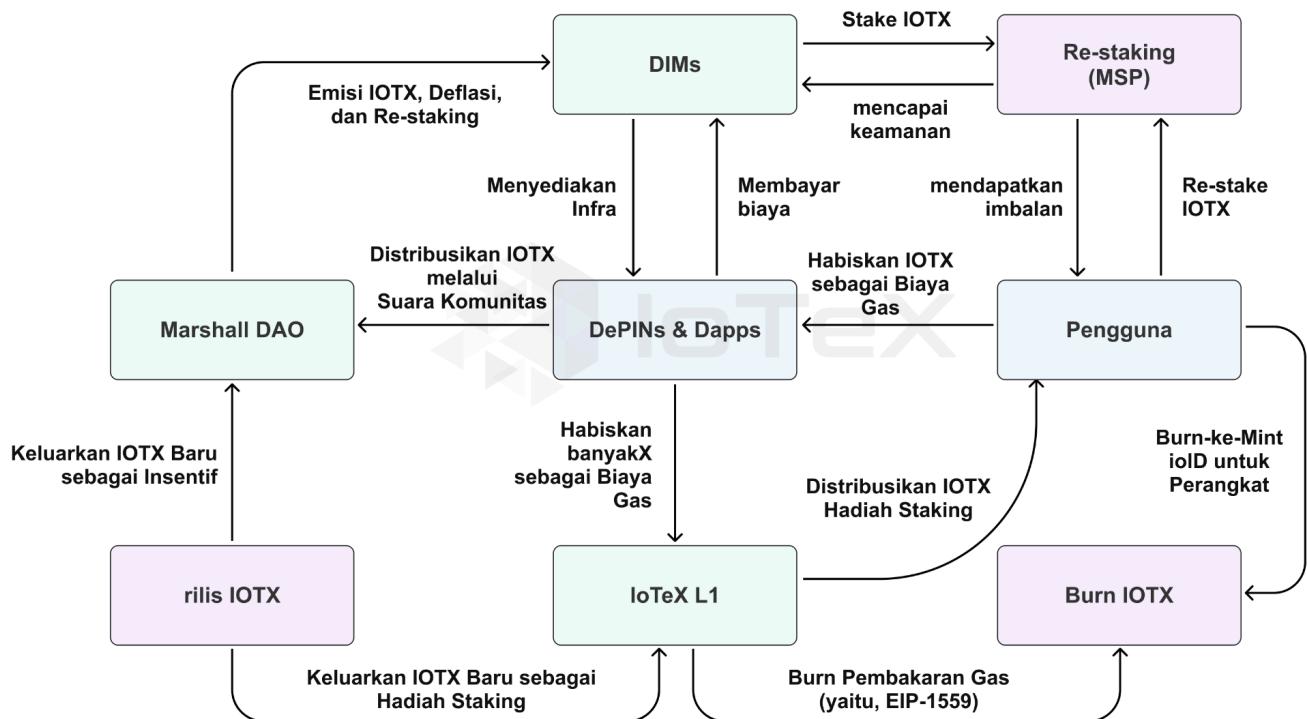
- **Dari Perspektif Modul Infrastruktur DePIN (DIM):** DIM akan diminta untuk melakukan staking IOTX agar dapat bergabung dengan Modular Security Pool (MSP), mendapatkan keamanan dari kumpulan aset yang dipertaruhkan ulang, dan menawarkan layanan mereka dengan cara yang dapat diverifikasi ke Dapps , L2, dan pengguna. DIM juga dapat memilih untuk menggunakan IOTX sebagai pembayaran dari Dapps yang memanfaatkan layanan mereka, atau mereka dapat menggunakan token mereka sendiri. Misalnya, penyedia penyimpanan jangka panjang seperti Filecoin atau penyedia ketersediaan data seperti NEAR akan

mempertaruhkan IOTX untuk bergabung dengan IoTeX 2.0 sebagai DIM, setelah itu mereka dapat membebankan biaya kepada Dapps untuk layanan data mereka dalam token mereka sendiri. Untuk beberapa DIM IoTeX 2.0 yang dibuat sendiri oleh tim IoTeX, seperti ioID dan ioConnect, pembayaran untuk layanan ini akan dalam mata uang token IOTX.

- **Dari Perspektif DePIN Dapps & DePIN L2s:** Dapps dan L2 yang diluncurkan pada tumpukan teknologi IoTeX 2.0 akan membayar IOTX untuk memproses transaksi dan berinteraksi dengan kontrak pintar. Selain itu, rantai Dapps dan L2 dapat memilih tumpukan teknologi modular mereka sendiri dan membayar satu atau lebih DIM untuk layanan, seperti konektivitas, penyimpanan data, komputasi off-chain, dan banyak lagi, dalam token DIM. Sebagai penutup, sebagian besar Dapps akan memiliki tokennya sendiri yang akan diperoleh dan dibelanjakan pengguna untuk mengakses layanan Dapps.

Selain utilitas token IOTX di atas, terdapat juga desain baru untuk IoTeX 2.0 mengenai bagaimana token IOTX akan dibakar berdasarkan penggunaan infrastruktur, bagaimana IOTX akan dibagikan dengan Dapps dan pembangun melalui program insentif, dan bagaimana IOTX baru akan digunakan. akan dipancarkan ke pemangku kepentingan di masa depan, seperti yang ditunjukkan pada Gambar 2.5. Kami mengeksplorasi desain baru ini di subbagian berikut.

Penerbitan IOTX, deflasi, dan re-staking



Gambar 2.5: Emisi, Deflasi, dan Pengambilan Ulang Token IOTX di IoTeX 2.0

2.3.2 Imbalan Staking Inflasi

Ketika Mainnet IoTeX diluncurkan pada tahun 2019, 12% dari total pasokan IOTX (yaitu, 1,2 miliar IOTX) dialokasikan untuk mempertaruhkan hadiah bagi Delegasi. Pemegang token melakukan staking IOTX untuk memilih Delegasi yang berbagi sebagian dari hadiah staking dengan pemilih mereka. Sejak 2019, sekitar 200 juta IOTX per tahun telah didistribusikan kepada Delegasi dan pemilih dalam bentuk block rewards dan epoch rewards. Hadiah blok diberikan kepada Delegasi Konsensus (yaitu, 36 Delegasi terpilih teratas yang memenuhi syarat untuk memproduksi blok) untuk setiap blok baru yang diproduksi, sementara hadiah epoch dibagi secara proporsional ke 100 Delegasi terpilih teratas setiap epoch (yaitu, setiap jam). Setelah lebih dari 4 tahun Mainnet aktif, pasokan IOTX yang awalnya dialokasikan untuk hadiah staking hampir didistribusikan sepenuhnya. Oleh karena itu, imbalan staking yang bersifat inflasi akan diperkenalkan sebagai bagian dari IoTeX 2.0 untuk memberi insentif kepada Delegasi agar terus memvalidasi transaksi jaringan dan mengamankan jaringan.

Imbalan staking yang bersifat inflasi didefinisikan sebagai IOTX baru yang ditambahkan ke pasokan token, dikirimkan kepada Delegasi yang berpartisipasi dalam konsensus dan pemegang token yang melakukan staking IOTX. Pada dasarnya, ini berarti hanya mereka yang melakukan staking token IOTX yang akan menerima token IOTX yang baru dibuat, sehingga mendorong rasio staking IOTX yang lebih tinggi dan keamanan yang lebih tinggi untuk jaringan IoTeX secara keseluruhan. Distribusi imbalan staking yang bersifat inflasi akan mengikuti struktur yang sama dengan distribusi IOTX sebelumnya yang dialokasikan untuk imbalan staking, di mana Delegasi Konsensus yang memproduksi blok akan memperoleh imbalan blok dan 100 Delegasi Teratas akan membagi imbalan epoch secara proporsional.

Meskipun ini adalah konsep baru untuk Jaringan IoTeX, imbalan staking yang bersifat inflasi sudah ada di hampir semua L1, termasuk Ethereum, Solana, Cosmos, dan banyak lagi. Misalnya, Solana memulai dengan tingkat inflasi 8%, yang berkurang 15% setiap tahunnya; pada Q1 2024, Jaringan Solana mengalami inflasi sebesar ~5,5%. Meskipun persentase sebenarnya dari inflasi tahunan untuk Jaringan IoTeX akan ditentukan oleh tata kelola seluruh jaringan, tujuannya adalah untuk memperkenalkan inflasi ringan yang memberikan APR imbalan staking yang kompetitif untuk delegasi IoTeX L1 dibandingkan dengan ekosistem blockchain lainnya, dan memberikan insentif kepada DIM dan Aplikasi DePIN akan berkembang sambil mempertahankan pasokan token yang stabil ketika memperhitungkan pembakaran token yang bersifat deflasi, yang dirinci pada bagian di bawah ini.

2.3.3 Pembakaran Deflasi

Untuk menyeimbangkan inflasi yang diperlukan dalam jaringan kripto, pembakaran token secara deflasi berdasarkan penggunaan jaringan biasanya diterapkan untuk menjaga pasokan token tetap stabil (misalnya, Burn and Mint Equilibrium adalah pola desainnya). Misalnya, Jaringan Ethereum mengeluarkan sekitar 1.700 ETH baru per hari kepada validator, namun menyeimbangkan inflasi ini dengan pembakaran biaya bahan bakar yang bersifat deflasi (yaitu, EIP-1559) untuk mempertahankan pasokan token ETH yang stabil atau deflasi secara keseluruhan dari waktu ke waktu. Sejak tahun 2020, Jaringan IoTeX memanfaatkan program Burn-Drop untuk mendorong pembakaran IOTX secara deflasi berdasarkan jumlah perangkat baru yang terdaftar ke jaringan, yang

mengakibatkan sekitar 4% dari total pasokan atau 400 juta IOTX dibakar hingga saat ini. Dengan diperkenalkannya IoTeX 2.0 dan penghentian program Burn-Drop, sumber pembakaran deflasi baru akan ditambahkan ke Jaringan IoTeX di tingkat protokol berdasarkan penggunaan infrastruktur modular kami.

- Pada tingkat L1, IoTeX 2.0 akan memperkenalkan pembakaran biaya bahan bakar yang mirip dengan EIP-1559 Ethereum. Hal ini akan memberikan insentif dan mendistribusikan kembali nilai kepada pemegang token IOTX berdasarkan peningkatan penggunaan IoTeX L1. Taruhan IOTX untuk berpartisipasi dalam tata kelola dan memilih Delegasi akan tetap tidak berubah, mempertahankan efek penting dari aset yang dipertaruhan yang mengurangi kecepatan token IOTX.
- Di IoTeX 2.0, ioID akan didaftarkan ke IoTeX L1 dan satu atau lebih VC untuk perangkat akan diperoleh dengan membakar token IOTX untuk mengakses DIM seperti W3bstream. Desain ini akan mendistribusikan kembali nilai kepada pemegang token IOTX berdasarkan pertumbuhan jumlah perangkat yang "dilengkapi" di Jaringan IoTeX, mirip dengan Burn-Drop tetapi didesain ulang agar lebih selaras dengan desain modular IoTeX 2.0. Di IoTeX 2.0, ioID akan didaftarkan ke IoTeX L1 dan satu atau lebih VC untuk perangkat akan diperoleh dengan membakar token IOTX untuk mengakses DIM seperti W3bstream. Desain ini akan mendistribusikan kembali nilai kepada pemegang token IOTX berdasarkan pertumbuhan jumlah perangkat yang "dilengkapi" di Jaringan IoTeX, serupa dengan Burn-Drop namun didesain ulang agar lebih selaras dengan desain modular IoTeX 2.0.
- Untuk W3bstream, ioConnect, dan ioDDK, efek jaringan yang dipicu oleh pertumbuhan dan adopsi produk modular ini oleh Dapps dan perusahaan akan mendorong pembakaran IOTX secara deflasi karena kebutuhan perangkat untuk berinteraksi langsung dengan masing-masing DIM. Selain itu, pembakaran token IOTX secara berkala berdasarkan ambang adopsi yang ditentukan oleh komunitas IoTeX dapat dilakukan untuk mendistribusikan kembali nilai kepada pemegang token.

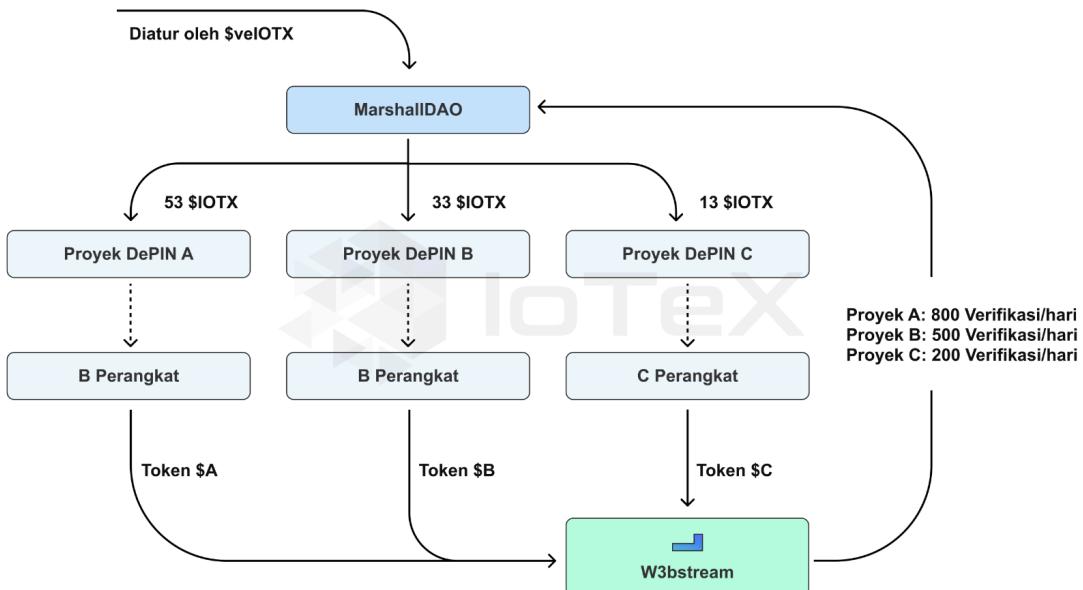
Tokenomik IoTeX 2.0 dirancang untuk menghargai peningkatan penggunaan berbagai komponen modular platform IoTeX dengan mendorong pembakaran token IOTX secara deflasi. Pada awalnya, pembakaran deflasi ini akan mengimbangi imbalan staking yang bersifat inflasi yang disebutkan di atas untuk mempertahankan total pasokan token bersih yang stabil, dan di masa depan adopsi massal platform IoTeX dapat mendorong

total pasokan token IOTX menjadi deflasi bersih. Untuk mendorong adopsi massal yang diperlukan untuk mencapai hal ini, tokennomics IoTeX 2.0 akan mengalokasikan token IOTX ke berbagai pembangun melalui program insentif pertumbuhan yang dijelaskan di bawah ini.

2.3.4 Insentif Pertumbuhan

Pilar penting IoTeX 2.0 adalah Marshall DAO (IIP-23) [10], sebuah Organisasi Otonomi Terdesentralisasi (DAO) yang akan memungkinkan pemangku kepentingan IoTeX membuat proposal mengenai bagaimana mengalokasikan insentif IOTX untuk menumbuhkan ekosistem IoTeX, termasuk memasukkan proyek DePIN yang bereputasi baik dan mendanai inisiatif jaringan luas. Hal ini menciptakan sistem yang transparan dan meritokratis di mana ide-ide terbaik didanai menggunakan IOTX. Marshall DAO pada awalnya akan didanai oleh lebih dari 500 juta IOTX yang digunakan kembali dari alokasi Burn-Drop, yang diputuskan oleh komunitas IoTeX melalui pemungutan suara di seluruh jaringan pada Q1 2024. Di masa depan, pendanaan tambahan untuk Marshall DAO mungkin ditambahkan melalui pemungutan suara lebih lanjut di seluruh jaringan untuk menambahkan IOTX baru ke kumpulan.

Seperti yang ditunjukkan pada Gambar 2.6, Marshall DAO menggunakan model tata kelola on-chain vote-escrow, yang berarti semakin banyak IOTX yang dipertaruhkan di DAO, semakin besar hak suara yang dimiliki pengguna. Hal ini memastikan keputusan untuk mendanai proyek dan inisiatif dibuat oleh mereka yang paling banyak berinvestasi dalam kesuksesan jangka panjang IoTeX. Pemegang token yang melakukan staking setidaknya selama 91 hari akan mendapatkan veIOTX, token on-chain yang tidak dapat dipindah tangankan, yang dapat digunakan untuk mengusulkan dan memberikan suara pada alokasi pendanaan melalui alat ukur yang mewakili proposal tertentu. Ini berarti pemangku kepentingan jangka panjang dapat memberikan suara menggunakan veIOTX mereka untuk membentuk bagaimana IOTX dari DAO mendanai berbagai proyek, termasuk namun tidak terbatas pada meningkatkan likuiditas untuk pasangan dagang DEX di IoTeX, mensponsori proyek DePIN tahap awal melalui landasan peluncuran, mempercepat De- Proyek PIN melalui penambangan ganda, pemberian hibah untuk barang publik dan alat di seluruh jaringan, dan banyak lagi.

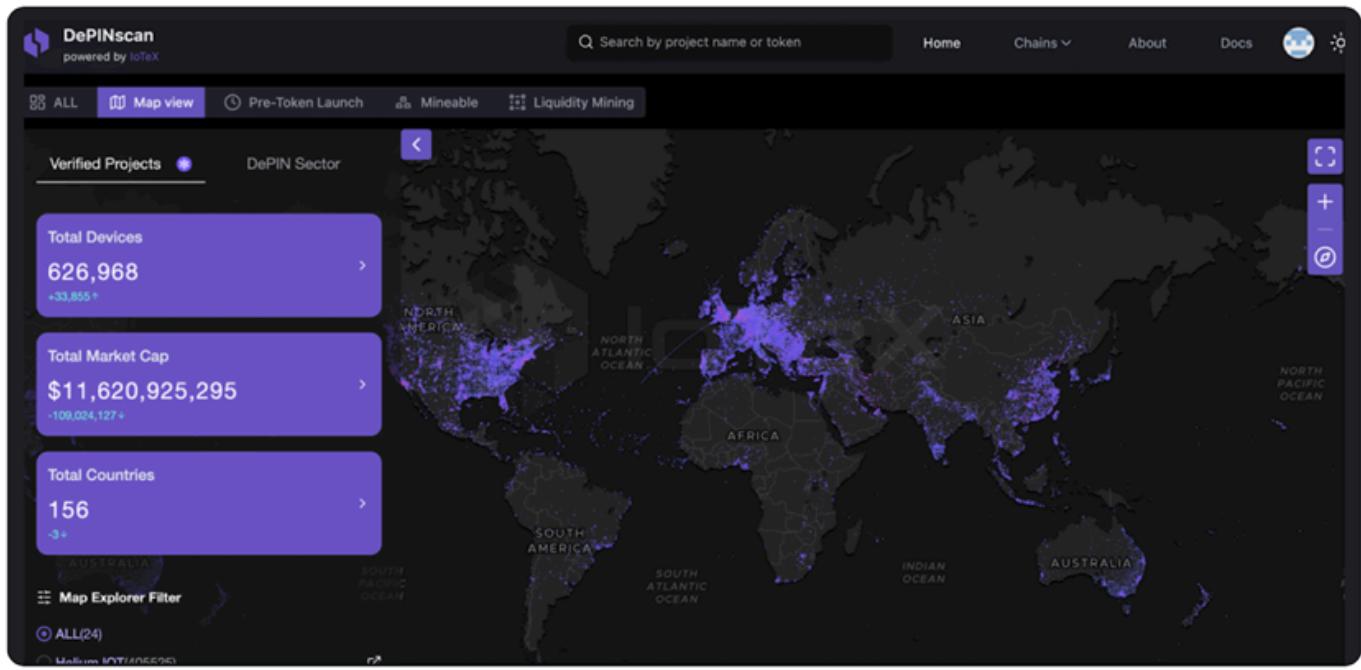


Gambar 2.6: Model Tata Kelola Marshall DA

2.4 Barang Publik

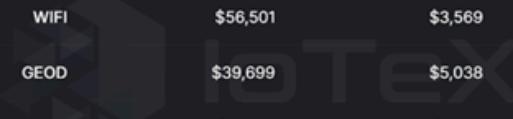
Selain kemampuan yang disediakan oleh blockchain dan DIM IoTeX, barang publik yang mengatasi banyak tantangan jangka pendek dan menengah dari proyek De-PIN juga merupakan bagian penting dari IoTeX 2.0. Barang publik ini memberikan kesadaran, kegunaan, dan likuiditas pada proyek DePIN melalui integrasi sederhana, serta memberikan komunitas IoTeX cara untuk memantau industri DePIN yang lebih luas serta mendalami proyek tertentu.

- DePINScan [23] adalah penjelajah industri untuk sektor DePIN (lihat Gambar 2.7). Ini dirancang untuk memberdayakan pengguna, penambang, dan investor di DePIN untuk memantau pertumbuhan proyek DePIN dan menemukan proyek tahap awal. Ini memberikan jumlah perangkat dan profil proyek secara real-time, berfungsi sebagai cara untuk menemukan proyek dan mendapatkan harga, volume, dan kapitalisasi pasar real-time untuk aset DePIN.



Gambar 2.7: Penjelajah DePINScan

- DePIN Liquidity Hub [21] adalah DEX tipe Uniswap v3 dengan likuiditas terkonsentrasi yang menyediakan range manager otomatis (pembuat pasar) dan memungkinkan pengguna untuk memperdagangkan token DePIN (lihat Gambar 2.8). Likuiditas token sangat penting bagi proyek kripto apa pun, terutama DePIN, karena mereka banyak menggunakan token mereka sebagai mekanisme insentif untuk mengembangkan jaringan mereka. Sayangnya, banyak DePIN tahap awal kesulitan menciptakan dan mempertahankan tingkat likuiditas on-chain yang sehat. Untuk mendukung proyek baru, IoTeX telah meluncurkan DePIN Liquidity Hub [24] untuk meningkatkan likuiditas proyek DePIN yang dapat menjembatani token mereka dari rantai L1 lainnya ke IoTeX L1, menciptakan kumpulan likuiditas dua sisi di berbagai bursa terdesentralisasi (DEX), dan menjalankan kampanye penambangan likuiditas untuk memberi insentif kepada investor agar meningkatkan likuiditas on-chain mereka.



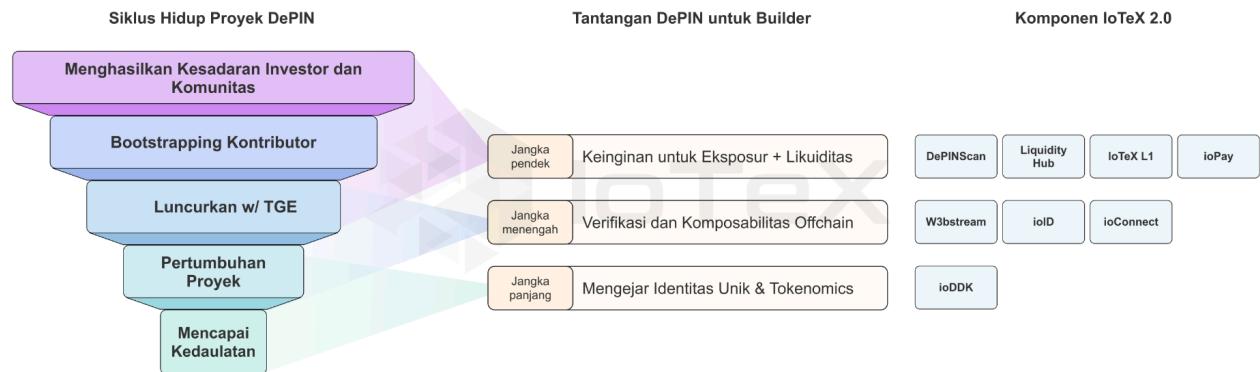
Top Tokens	DePIN Tokens					See All
Name	Symbol	Liquidity ↓	Volume (24hrs)	Price	Price Change (24hrs)	
1 Wrapped IOTX	WIOTX	\$13,948,780	\$95,531	\$0.0463	+4.34%	
2 WEN	WEN	\$1,473,287	\$5,274	\$1.03	+2.86%	
3 Dimo	DIMO	\$146,790	\$1,812	\$0.47	+4.00%	
4 Wifi Map	WIFI	\$56,501	\$3,569	\$0.13	+24.56%	
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	+7.61%	
9 XNet Mobile	XNET	\$16,383	\$302.29	\$0.0366	-2.77%	
10 DRIFE	DRF	\$12,050	\$1,229	\$0.0024	-3.81%	

Gambar 2.8: Pusat Likuiditas DePIN

Selain barang publik di atas yang sudah tersedia untuk para pembangun, ada barang lain yang akan dibangun oleh tim IoTeX serta pembangun global selama pengembangan IoTeX 2.0. Contohnya adalah landasan peluncuran proyek DePIN untuk membawa proyek mereka ke investor yang berminat, pasar perangkat untuk mengekspos perangkat keras yang berfokus pada DePIN kepada para penambang, dan alat tata kelola untuk memungkinkan pemungutan suara terdesentralisasi untuk proyek DePIN. Dengan tersedianya barang publik bagi para pembangun, IoTeX 2.0 akan memberdayakan proyek dengan serangkaian kemampuan lengkap untuk membuat peluncuran dan pengembangan proyek DePIN menjadi lebih mudah dari sebelumnya.

2.5 Mendukung Pembangun Sepanjang Siklus Hidup Proyek

IoTeX 2.0 menawarkan beragam infrastruktur, alat, dan sumber daya publik, semuanya diatur oleh tokenomics meritokratis. Ini dirancang untuk membantu pembangun DePIN di setiap fase siklus hidup proyek mereka, seperti yang ditunjukkan pada Gambar 2.9.



Gambar 2.9: Pembangun Dukungan di seluruh Siklus Hidup Proyek DePIN

- Pada tahap awal, proyek DePIN terutama berfokus pada pengembangan tumpukan teknologi dan menciptakan kesadaran akan proyek mereka. Untuk memfasilitasi hal ini, IoTeX 2.0 menyediakan sumber daya publik seperti DePINscan dan Liquidity Hub untuk menarik perhatian, likuiditas, dan pengguna.
- Seiring dengan kemajuan proyek, permintaan akan infrastruktur yang lebih maju dan mudah beradaptasi meningkat, terutama karena proyek-proyek tersebut mendesentralisasikan tumpukan teknologi mereka dan bertujuan untuk meningkatkan skalabilitas. Untuk memenuhi kebutuhan ini, IoTeX 2.0 menawarkan infrastruktur seperti W3bstream, IoID, dan IoConnect untuk menyediakan teknologi mutakhir bagi pembuat DePIN
- Dalam jangka panjang, proyek-proyek DePIN perlu membangun dan memperluas jaringan pasokan dan permintaan mereka sendiri. IoTeX 2.0 terus mendukung

proyek-proyek ini bahkan pada tahap selanjutnya dengan memungkinkan mereka meluncurkan L2 mereka sendiri melalui ioDDK.

2.6 Masa Depan

Dengan IoTeX 2.0, kami memulai perjalanan baru untuk melengkapi perangkat dunia dengan semua alat yang mereka perlukan agar dapat berdaulat, mengumpulkan intelijen dunia nyata untuk mendukung Dapps yang inovatif, dan memungkinkan pengguna untuk memonetisasi layanan unik dan intelijen dari perangkat mereka. perangkat. Konvergensi kecerdasan buatan, blockchain, dan perangkat pintar yang sedang berlangsung kini memicu revolusi teknologi yang secara mendasar akan mengubah cara dunia bekerja. Meskipun teknologi-teknologi ini telah berkembang secara independen dari waktu ke waktu, teknologi-teknologi tersebut menjadi semakin saling terkait dan dikemas menjadi sebuah aset produktif baru: jaringan DePIN terdiri dari perangkat-perangkat tepercaya dan milik pengguna.

Perangkat pintar akan menyediakan layanan dan menghasilkan data. Blockchain akan menambah kepercayaan dan verifikasi pada data dan layanan ini. Dan terakhir, AI akan mengambil nilai dari data dan mengotomatiskan layanan ini Apa yang tampak seperti fiksi ilmiah beberapa tahun yang lalu kini menjadi kenyataan. Dalam waktu dekat, perekonomian mesin yang sedang berkembang akan didorong oleh trinitas teknologi ini dan menjadi industri paling bernilai di dunia. Dengan blockchain, kita akan memiliki kemampuan untuk memprogram ekonomi mesin baru ini dengan teknologi tepercaya yang tidak hanya bermanfaat bagi masyarakat tetapi juga memberikan nilai dan kesetaraan bagi masyarakat sehari-hari. Kemungkinannya tidak terbatas, namun beberapa peluang yang paling menarik adalah:

- **Kecerdasan Kolektif & AI:** IoTeX akan menjadi pusat perangkat terbesar, dan juga pusat data dunia nyata, untuk mengumpulkan informasi waktu nyata. Dengan menangkap aliran data dari perangkat dan memverifikasi peristiwa dunia nyata secara on-chain, kita dapat mengumpulkan kecerdasan kolektif masyarakat untuk merevolusi industri individual seperti konektivitas, kota pintar, dan energi terbarukan. Peluang yang lebih besar lagi terletak pada pemanfaatan AI untuk menganalisis hubungan lintas industri dan mengekstrak wawasan relasional yang

dapat mengembangkan pemahaman kita tentang dunia. IoTeX 2.0 akan menjadi platform terdesentralisasi yang mencatat sejarah dunia nyata melalui perangkat pintar kita, memungkinkan kita memahami masa lalu sehingga kita dapat mengoptimalkan masa depan.

- **Ekonomi Mesin Otonom:** Selain menghasilkan data berharga, perangkat pintar kini berevolusi untuk memberikan layanan tepercaya dan berharga bagi masyarakat. Taksi otonom menghadirkan kendaraan tanpa pengemudi yang pertama, satelit menyediakan konektivitas kepada masyarakat di seluruh dunia, gudang menggunakan robot yang melebihi ketangkasannya manusia, dan energi matahari dan angin dihasilkan oleh perangkat energi terbarukan generasi berikutnya. Orkestrasi perangkat penyedia layanan ini paling baik dilakukan dengan blockchain dan AI yang cerdas. Kami membayangkan masa depan di mana IoTeX dapat memungkinkan sistem AI memantau dan mengelola sumber daya bumi dengan presisi dan kepercayaan penuh yang belum pernah ada sebelumnya.
- **Pasar Sumber Daya Digital:** Meskipun beberapa DePIN memfokuskan data dan layanan dari perangkat keras yang bergantung pada lokasi, DePIN lainnya mengumpulkan sumber daya digital dari perangkat keras agnostik lokasi. Hal ini dapat mencakup penyimpanan digital, komputasi melalui CPU dan GPU, bandwidth, dan sumber daya digital lainnya yang biasanya ditawarkan oleh konglomerat Cloud. Di era dimana "data adalah sesuatu yang baru emas" dan "komputasi adalah minyak baru", IoTeX 2.0 akan memungkinkan crowdsourcing sumber daya digital yang berharga ke pasar tempat siapa pun dapat bertukar mereka secara peer-to-peer dengan orang lain di seluruh dunia.
- **Tata Kelola & Pengambilan Keputusan yang Terdesentralisasi:** Dengan mengintegrasikan dunia nyata memasukkan data ke dalam blockchain dengan aman dan transparan, IoTeX 2.0 dapat membantu membangun fondasi pengambilan keputusan yang terdesentralisasi menggunakan fakta yang dapat diverifikasi tentang kejadian di dunia nyata. Dengan manusia secara kolektif mendefinisikan proses melalui tata kelola yang terdesentralisasi, kita dapat memanfaatkan kontrak pintar yang tidak dapat diubah dan perangkat yang aman untuk mengoperasikan aspek-aspek utama masyarakat dengan cara yang tepercaya. IoTeX 2.0 memberikan jalan bagi siapa saja untuk menyumbangkan keahlian dan keahliannya berpartisipasi dalam pemerintahan terbuka di dunia baru.

Bagian 3

Modular Security Pool (MSP) - Lapisan Tepercaya Terpadu untuk Modul Infrastruktur DePIN

3.1 Masalahnya

DePIN menampilkan tumpukan teknologi komprehensif yang mencakup elemen on-chain seperti DePIN L2 spesifik skenario dan elemen off-chain seperti aliran data, oracle, proses, verifikasi, penyimpanan, dan otomatisasi. Struktur kompleks ini memerlukan lebih banyak modul dan pembangun untuk membuat arsitektur kepercayaan terdesentralisasi mereka sendiri dari awal. Tugasnya mungkin termasuk merancang token staking, menciptakan likuiditas, menarik pemangku kepentingan, merekrut validator, dan mendapatkan adopsi pasar, yang mengarah pada potensi fragmentasi keamanan dan desentralisasi.

Untuk membangun kepercayaan terpadu dan menyeluruh dalam cara yang terdesentralisasi, penting untuk memastikan bahwa setiap bagian seaman dan terdesentralisasi, dengan mengikuti prinsip hubungan terlemah (weakest link). Ketika para pembangun terus mengembangkan Modul Infrastruktur (DIM) DePIN, menjaga integritas keamanan dan desentralisasi tanpa fragmentasi adalah sebuah prioritas. Pendekatan ini memungkinkan integrasi DIM dengan cepat ke dalam tumpukan teknologi yang ada untuk digunakan dalam proyek DePIN. Modular Security Pool (MSP) menyediakan lapisan kepercayaan terpadu yang mendukung DIM. Ia mengumpulkan keamanan staking dari berbagai L1/L2 yang sudah ada dan dapat meminjamkan keamanannya ke DIM baru dengan imbalan kompensasi. Sistem ini memungkinkan modul infrastruktur baru mendapatkan manfaat dari keamanan L1/L2 yang mendasarinya tanpa membangun infrastruktur keamanannya sendiri. Misalnya, DIM

baru dapat bergabung dengan MSP melalui proposal tata kelola. Jika disetujui, DIM akan mengadopsi keamanan dan desentralisasi L1/L2 dan menerima penggunaan protokol mereka dari proyek ekosistem IoTeX. Staker yang mendukung DIM tertentu dengan mengarahkan taruhannya ke MSP dapat menerima kompensasi dalam bentuk token jaringan DIM.

3.2 Pasar Terbuka untuk Keamanan dan Kepercayaan

MSP dengan penuh percaya diri menghadirkan mekanisme pasar terbuka, yang dengan ahli mengatur pasokan dan konsumsi keamanan yang dikumpulkan oleh para pemangku kepentingan dan DIM. MSP akan mengkonsolidasikan keamanan yang berfokus pada DePIN di seluruh DIM, alih-alih memecah-mecah keamanan di antara banyak DIM. Konkritnya, ada tiga jenis peserta dalam MSP:

- **DIM Builder** membuat DIM seperti DePIN L2 spesifik skenario, layanan off-chain seperti streaming data, oracle, pemrosesan (seperti tujuan umum, berbasis ZKP, berbasis TEE, dll.), penyimpanan data, otomatisasi (seperti otomatis modul pembayaran, umpan harga), identitas, dan otentikasi. Pembuat DIM harus memberikan insentif kepada para pemangku kepentingan untuk mengalokasikan aset mereka ke modul mereka. MSP akan menyediakan mekanisme suap untuk memastikan para pemangku kepentingan mendapatkan insentif yang cukup dari DIM.
- **Staker** adalah peserta jaringan yang mendelegasikan aset mereka dari blockchain yang sudah mapan ke satu atau lebih validator. Mereka berkontribusi terhadap keamanan jaringan tanpa harus menjalankan node sendiri. Sebagai imbalan atas delegasi mereka, mereka mendapatkan sebagian dari biaya dan imbalan jaringan. Strategis alokasi menentukan modul yang layak mendapatkan keamanan tambahan, dengan mempertimbangkan potensi pemotongan lebih lanjut. Para pemangku kepentingan memiliki untuk ikut serta dengan mengizinkan MSP untuk menerapkan kondisi pemotongan ekstra pada aset mereka, sehingga meningkatkan keamanan ekonomi. Penting untuk dicatat di sini bahwa infrastruktur MSP yang kami bangun adalah sumber terbuka dan akan dapat memanfaatkan keamanan dari IoTeX L1 dalam waktu dekat dan semua blockchain utama, termasuk Bitcoin, Ethereum, dan Solana di masa depan.

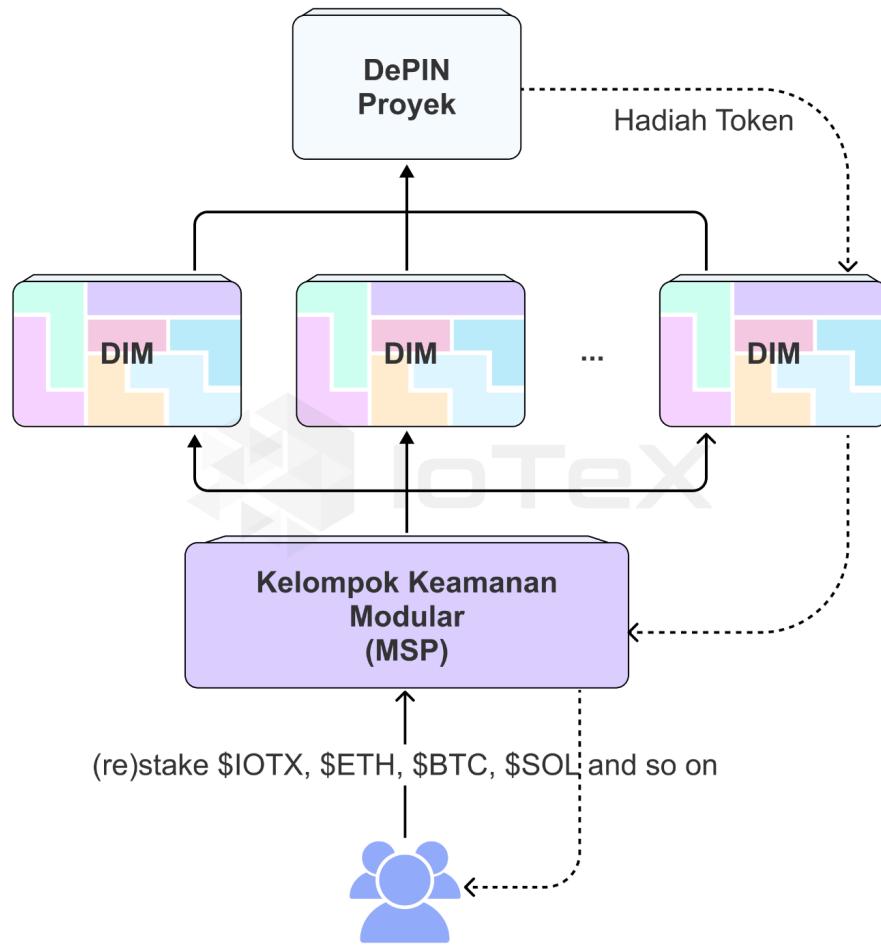
- **Validator** menyediakan kumpulan node yang selalu berjalan dan tersedia untuk build DIM- ers yang akan langsung melayani proyek DePIN.

Implementasi MSP harus memasukkan prinsip-prinsip utama berikut:

- **Terbuka masuk dan keluar:** Staker dan DIM harus memiliki kebebasan untuk masuk dan keluar pasar tanpa batasan apa pun. Hal ini memastikan harga yang kompetitif, mencerminkan nilai sebenarnya dari layanan.
- **Efek jaringan:** Ketika jumlah peserta meningkat, setiap peserta merasa pasar menjadi lebih bernilai. Umpam balik positif ini dapat menarik lebih banyak pembeli dan penjual ke pasar.
- **Tanpa Izin:** Pasar tidak dikendalikan oleh otoritas pusat. Di dalam- sebaliknya, ia beroperasi berdasarkan hukum penawaran dan permintaan.

3.3 Arsitektur

Seperti yang ditunjukkan pada Gambar 3.1, arsitektur Modular Security Pool (MSP) dirancang untuk menyediakan proses yang efisien dan aman untuk membangun jaringan baru, khususnya DePIN dan DIM, berdasarkan keamanan yang diwarisi dari sistem staking yang ada pada blockchain L1 yang sudah mapan. Berikut rincian rinci tentang cara kerja MSP:



Gambar 3.1: Arsitektur Modular Security Pool (MSP)

1. **Staker Mendelegasikan Aset:** Staker, yang merupakan peserta dalam L1 yang sudah mapan seperti Bitcoin, Ethereum, dan IoTeX, mendelegasikan aset mereka ke MSP. Dengan melakukan hal ini, mereka berkontribusi terhadap keamanan jaringan yang didukung MSP.
2. **Staker Memilih Validator:** Dalam jaringan MSP, staker memiliki fleksibilitas untuk memilih validator dari kumpulan opsi yang disediakan oleh jaringan DIM yang terkait dengan mereka. Validator bertanggung jawab menjalankan node untuk mengamankan jaringan dan memvalidasi transaksi.
3. **Validator Menjalankan Node:** Setelah dipilih oleh pemangku kepentingan, validator mengoperasikan node dalam jaringan MSP. Node-node ini memainkan peran penting dalam mem
4. **Pembangun DIM Membangun Jaringan:** Sementara itu, pembangun DIM sedang mengerjakan mengembangkan jaringannya masing-masing.

5. **Memberi Insentif kepada Staker:** Pembuat DIM memberi insentif kepada para pemangku kepentingan untuk mengalokasikan aset mereka ke modul mereka dalam jaringan MSP. Insentifikasi ini bisa dalam berbagai bentuk, seperti reward, token jaringan, atau manfaat lainnya. MSP memastikan bahwa para pemangku kepentingan mempunyai motivasi yang cukup melalui mekanisme seperti mekanisme suap untuk mendorong partisipasi.
6. **Distribusi Keamanan Staking:** MSP memainkan peran penting dalam mendistribusikan keamanan staking ke DIM baru. Dengan memanfaatkan keamanan gabungan yang dikumpulkan dari L1/L2 yang sudah ada dan partisipasi pemangku kepentingan dan validator, MSP melayani keamanan dan desentralisasi jaringan baru ini.

Secara keseluruhan, arsitektur ini memfasilitasi proses yang lebih efisien dan aman untuk meluncurkan DIM baru. Dengan memanfaatkan keamanan L1/L2 yang ada dan mengintegrasikan berbagai pemangku kepentingan seperti pemangku kepentingan, validator, dan pembangun, MSP menumbuhkan ekosistem kuat yang kondusif bagi inovasi dan pertumbuhan arsitektur kepercayaan yang terdesentralisasi. Pendekatan ini tidak hanya menghemat waktu dan sumber daya bagi pengembangan jaringan baru tetapi juga memperkuat keamanan dan ketahanan ekosistem DePIN secara keseluruhan.

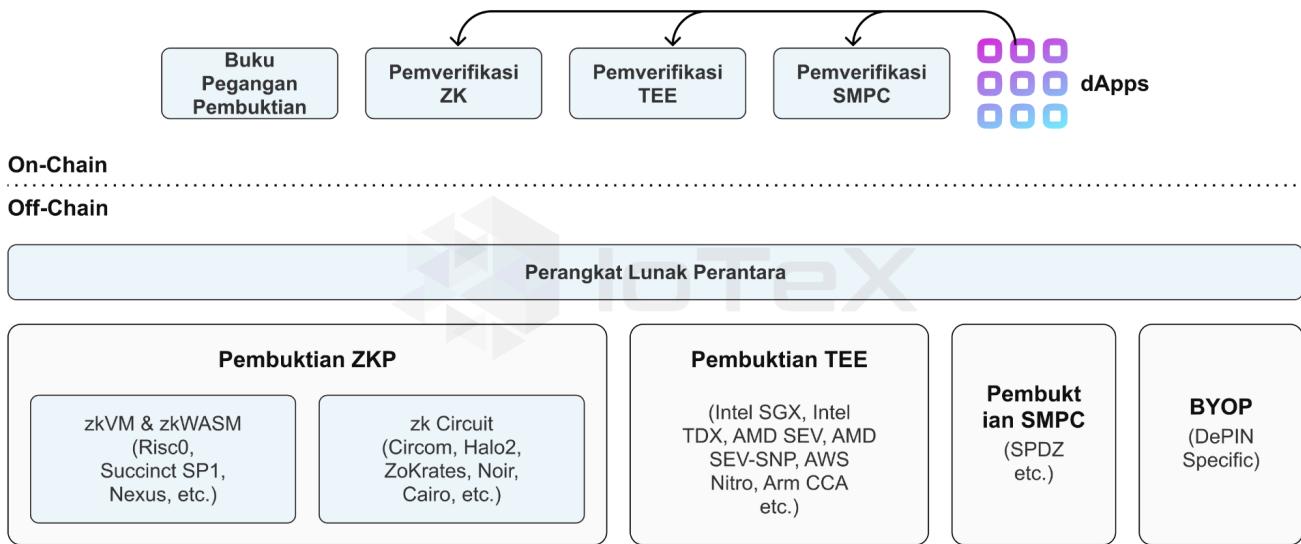
Bab 4

W3bstream - Jaringan Multi-Prover Terdesentralisasi untuk Verifikasi DePIN

Aplikasi DePIN biasanya berisi skenario pemrosesan data khusus (misalnya, menghitung skor, menemukan lokasi perangkat, mendeteksi perangkat palsu, dll.) yang mampu mengekstrak wawasan berdasarkan data yang dikumpulkan oleh perangkat DePIN dari dunia nyata. Wawasan tersebut kemudian digunakan untuk memicu kontrak pintar untuk tindakan terkait token. Karena tingginya volume data mesin, pemrosesan dan penyimpanannya secara on-chain menjadi mahal dan tidak efisien. Hasilnya, komputasi off-chain muncul sebagai solusi yang menjanjikan untuk mengatasi tantangan skalabilitas di DePIN.

4.1 Arsitektur W3bstream

W3bstream adalah jaringan multi-prover yang diatur dengan blockchain yang dikembangkan oleh IoTeX, yang bertujuan untuk memanfaatkan kekuatan server heterogen berskala global untuk meningkatkan aplikasi DePIN yang sedang berkembang. Singkatnya, W3bstream adalah jaringan komputasi off-chain terdesentralisasi yang terdiri dari node heterogen melakukan perhitungan yang dapat diverifikasi, seperti yang diilustrasikan pada Gambar 4.1. Bukti yang dihasilkan oleh W3bstream diverifikasi dengan verifikator on-chain dan kemudian digunakan oleh DePIN dApps.



Gambar 4.1: Singkatnya W3bstream

4.1.1 Empat Jenis Provers

Sejumlah teknik telah dikembangkan di masa lalu untuk membuktikan integritas pemrosesan data dan memungkinkan verifikasi publik, termasuk bukti tanpa pengetahuan (ZKP), lingkungan eksekusi tepercaya (TEE), dan komputasi multi-pihak yang aman (SMPC). Teknologi ini bergantung pada berbagai asumsi keamanan dan mempunyai implikasi berbeda dalam praktiknya. W3bstream mampu mengakomodasi empat kategori prover untuk mewujudkan komputasi yang dapat diverifikasi untuk aplikasi DePIN, yaitu Prover zero-knowledge proof (ZKP), Prover lingkungan eksekusi tepercaya (TEE), Prover komputasi multi-pihak yang aman (SMPC) dan Bawa Milik Anda Sendiri Prover (BYOP), melalui lapisan middleware yang dirancang dengan baik.

- **ZKP Prover:** ZKP memperbolehkan satu pihak (yaitu, seorang pembuktii) untuk membuktikan kepada pihak lain (yaitu, seorang verifikator) bahwa suatu pernyataan adalah benar, tanpa mengungkapkan informasi tambahan di luar fakta bahwa pernyataan tersebut benar. ZKP harus memenuhi persyaratan formal berupa kelengkapan, kesehatan, dan pengetahuan nol, sehingga memungkinkan seseorang untuk membangun aplikasi yang tidak dapat dipercaya. Dalam praktiknya, pembuktian ZKP dapat direalisasikan menggunakan mesin virtual zero-knowledge tujuan umum (zkVM) atau sistem batasan yang disesuaikan (yaitu

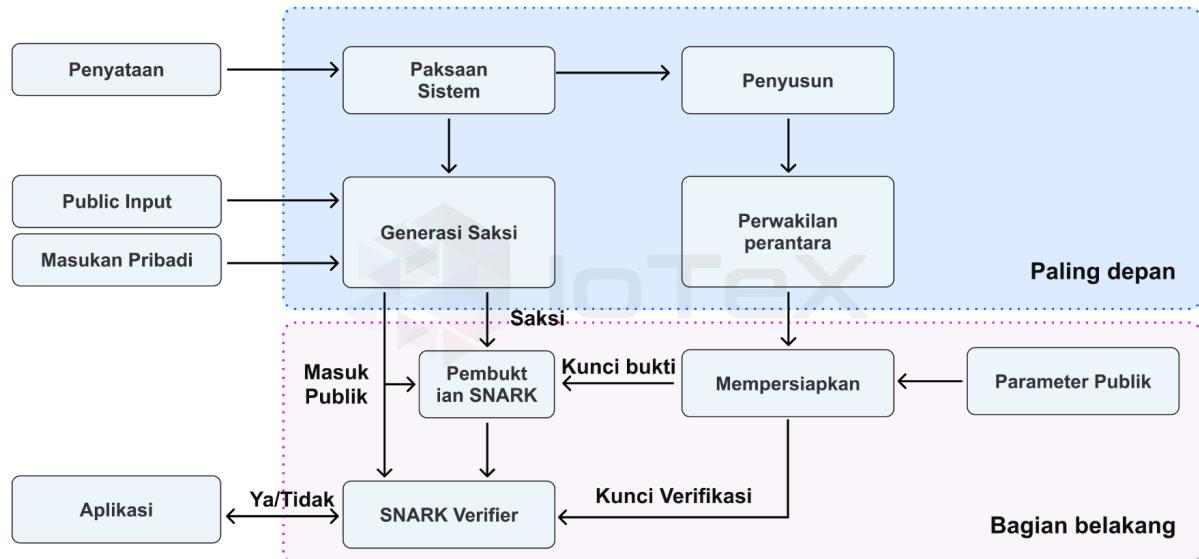
sirkuit). Arsitektur sistem khas dari aplikasi berbasis SNARK yang dibangun di atas zkVM (resp. sirkuit yang disesuaikan) diilustrasikan pada Gambar 4.2 dan 4.3.



Gambar 4.2: Arsitektur Sistem Aplikasi Berbasis SNARK yang Dibangun

sebuah zkVM

Sementara pembuktian berbasis zkVM untuk tujuan umum merangkum kompleksitas pembuatan ZKP dan memungkinkan pengembang mengkodekan logika bisnis mereka menggunakan bahasa pemrograman tingkat tinggi seperti C/C++, Rust, dll., membangun pembuktian ZKP dengan sirkuit yang disesuaikan memerlukan pemahaman yang lebih mendalam tentang alur kerja pembuatan ZKP serta bahasa khusus domain (DSL). Namun, pembuktian ZKP dengan sirkuit yang disesuaikan biasanya dapat mencapai kinerja yang lebih baik jika dibandingkan dengan pembuktian berbasis zkVM. Pembuktian ZKP memungkinkan pengembang DePIN memanfaatkan teknologi ZKP yang kuat untuk melakukan komputasi off-chain yang tidak dapat dipercaya. W3bstream secara bertahap akan mendukung proyek zkVM/zkWASM terkemuka (misalnya, Risc0 [28], Succinct SP1 [29], Nexus [30], zkWASM [31], dll.) serta DSL populer (misalnya, Circom [32], Halo2 [33], ZoKrates [34], Noir [35], Kairo [36], dll.) untuk membangun sirkuit zk yang disesuaikan.

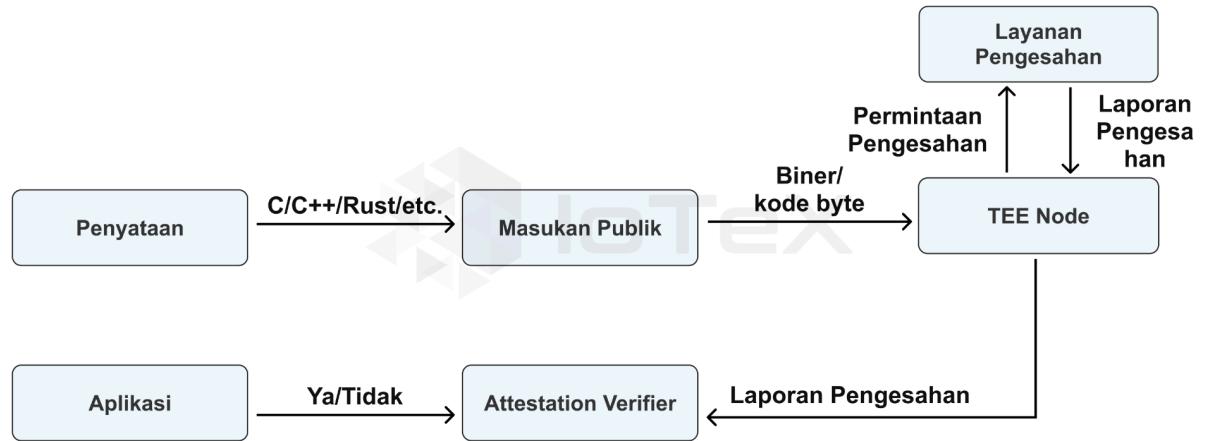


Gambar 4.3: Arsitektur Sistem Aplikasi Berbasis SNARK yang Dibangun pada Sirkuit yang Disesuaikan

- **Pepatah TEE:** Menurut definisi Confidential Computing Consortium (CCC), lingkungan eksekusi tepercaya (TEE) adalah lingkungan perangkat keras (dan perangkat lunak) khusus yang memberikan tingkat jaminan pada tiga properti berikut: 1) Kerahasiaan Data: Entitas yang tidak berwenang tidak dapat melihat data saat data tersebut digunakan dalam TEE; 2) Integritas Data: Entitas yang tidak berwenang tidak dapat menambah, menghapus, atau mengubah data saat data tersebut digunakan dalam TEE; dan 3) Integritas Kode: Entitas yang tidak berwenang tidak dapat menambah, menghapus, atau mengubah kode yang dijalankan di TEE. Properti keamanan yang menonjol ini memastikan kerahasiaan dan integritas data dan program, sehingga memungkinkan pihak jarak jauh memercayai hasil komputasi pada platform perangkat keras yang mendukung TEE (misalnya, Intel SGX, AMD-SEV, Arm CCA, AWS Nitro, NVIDIA H100 , dll.). Sistem berbasis TEE mengakarkan keamanannya pada perangkat keras dan pengguna harus percaya bahwa perangkat keras tersebut tidak mengalami kerusakan atau rusak secara tidak terdeteksi.

Arsitektur sistem yang khas dari aplikasi berbasis TEE ditunjukkan pada Gambar 4.4, yang bergantung pada mekanisme pengesahan jarak jauh dari platform perangkat keras berbasis TEE. Pengesahan jarak jauh adalah sebuah proses di mana satu pihak (yaitu, verifikator) menilai kelayakan dari rekan jarak jauh yang

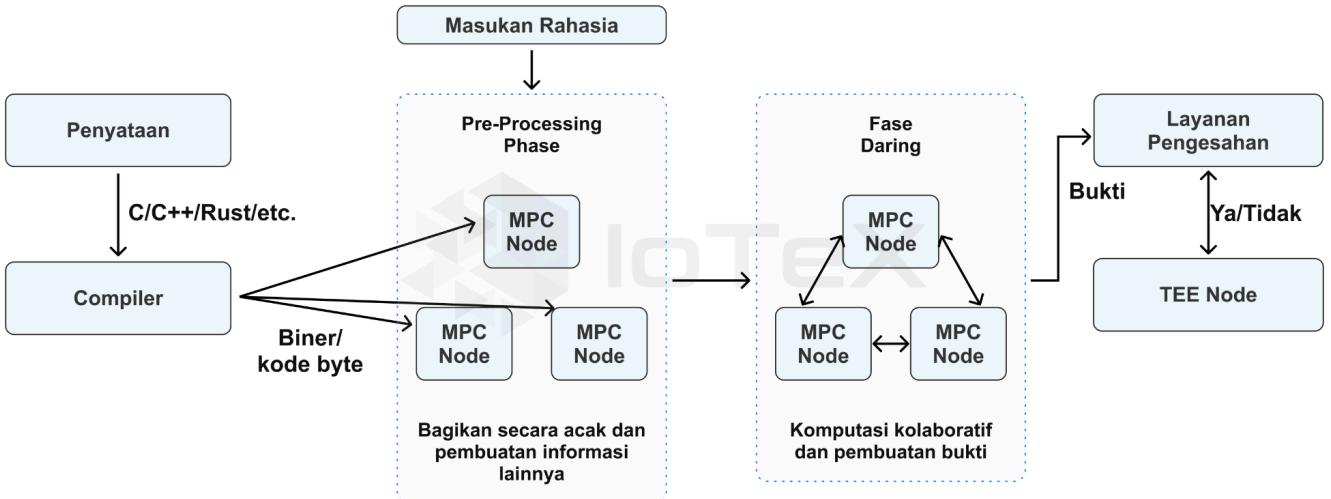
berpotensi tidak dapat dipercaya (yaitu, seorang penguji). Tujuan dari pengesahan adalah untuk memungkinkan verifikator mendapatkan keyakinan atas kepercayaan dari penguji dengan memperoleh laporan yang autentik, akurat, dan tepat waktu tentang perangkat lunak dan status data dari penguji. Dengan bantuan layanan pengesahan, laporan pengesahan dapat diperoleh yang berisi pengukuran kriptografi lingkungan eksekusi (yaitu, perangkat keras, perangkat lunak, data khusus, dll.).



Gambar 4.4: Arsitektur Sistem Aplikasi Berbasis TEE

Prover TEE dapat diterapkan dengan mengikuti perkembangan umum aliran penyedia TEE tertentu. Pembuktian TEE memfasilitasi pengembang DePIN untuk memanfaatkan teknologi komputasi rahasia yang canggih untuk melakukan komputasi off-chain yang menjaga privasi. W3bstream akan secara bertahap mendukung aliran pengembangan platform perangkat keras berbasis TEE terkemuka seperti Intel SGX [37], Intel TDX [38], AMD SEV [39], AMD SEV-SNP [40], AWS Nitro [41], Arm CCA [42], dll.

- **SMPC Prover:** MPC mewakili kumpulan teknik untuk menjaga privasi komputasi kolaboratif atas data terdistribusi dan tidak mengungkapkan apa pun selain itu hasil komputasinya. Mengingat berbagai asumsi dan ancaman keamanan model (misalnya, musuh semi-jujur, musuh jahat, iklan terselubung versaries), protokol SMPC setidaknya harus memenuhi tiga properti, yaitu privasi masukan, kebenaran dan independensi masukan. Arsitektur sistem tipikal aplikasi berbasis SMPC yang dibangun berdasarkan pra-pemrosesan model ditunjukkan pada Gambar 4.5.



Gambar 4.5: Arsitektur Sistem Aplikasi Berbasis SMPC

Pembuktian SMPC dapat diwujudkan dengan mengikuti alur pengembangan secara umum dari protokol SMPC tertentu (misalnya, SPDZ). Namun, mencapai kemampuan verifikasi publik dengan cara yang efisien masih merupakan arah penelitian yang berkelanjutan.

- **Bawa Prover Anda Sendiri (BYOP):** BYOP menawarkan fleksibilitas besar bagi pengembang De-PIN yang menerapkan prover yang dioptimalkan yang disesuaikan dengan proyek DePIN tertentu atau mengeksplorasi teknik komputasi baru yang dapat diverifikasi dan efisien dalam konteks DePIN.

4.1.2 Inovasi In-house Kami pada ZKP

Perkalian multi-skalar (MSM) adalah salah satu komponen inti dari banyak sistem pembuktian tanpa pengetahuan, dan merupakan penghambat kinerja utama dalam pembuatan bukti dalam skema ini. Salah satu strategi utama untuk mempercepat LSL adalah dengan memanfaatkan pra-komputasi. Beberapa algoritma (misalnya, Pippenger [11, 12] dan BGMW [13]) dan variannya telah diusulkan ke arah ini. Dalam penelitian terbaru kami [15], kami meninjau kembali metode penghitungan MSM berbasis

pra-perhitungan yang diusulkan oleh Luo, Fu, dan Gong di CHES 2023 [14] dan menggeneralisasi pendekatan mereka. Secara khusus, kami menyajikan konstruksi umum bucket yang optimal. Peningkatan ini menghasilkan peningkatan kinerja sekitar 15% ~ 40%, yang diverifikasi oleh analisis teoretis dan eksperimen. Kami juga memperkenalkan perekaman yang dapat diterima dalam bucket menggunakan endomorfisme cepat pada kurva elips $j = 0$ untuk membagi kebutuhan penyimpanan dengan 3, hampir tanpa penalti kinerja, dibandingkan dengan algoritma LFG kami yang sudah dioptimalkan.

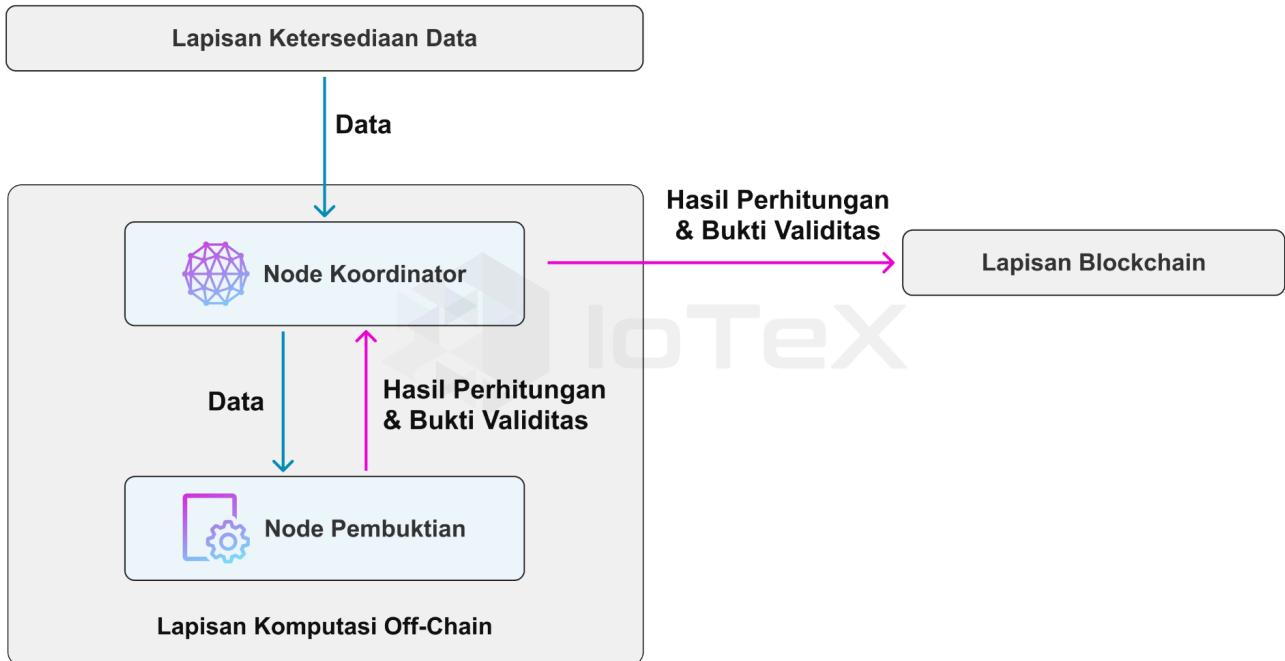
4.2 Alur Kerja W3bsteam

4.2.1 Orientasi dan Manajemen Prover

Orientasi pembuktian didasarkan pada ioID dan mengikuti proses yang dijelaskan dalam Bagian 5.2.2 - Pendaftaran dan Pengikatan ioID. Kontrak manajemen armada on-chain bertanggung jawab untuk menjadwalkan tugas dan melacak siklus hidup semua node pembuktian. Setiap node pembuktian dapat berstatus 'Sibuk', 'Idle', atau 'Offline' dan status node akan terus diperbarui dalam kontrak manajemen armada. Penjelajah W3bstream dapat digunakan untuk memeriksa status semua node pembuktian.

4.2.2 Alur Kerja

Dalam infrastruktur DePIN modular, W3bstream merupakan implementasi dari lapisan komputasi off-chain (OCCL) yang menampilkan beberapa pembuktian seperti yang dijelaskan dalam Bagian 4.1. W3bstream adalah kumpulan pembuktian heterogen terdesentralisasi yang mampu melakukan logika bisnis spesifik proyek pada data yang disimpan di lapisan ketersediaan data (DAL) dan menghasilkan bukti validitas (misalnya, bukti tanpa pengetahuan, laporan pengesahan, dll.) dari perhitungan yang dijalankan. W3bstream bekerja sebagai komponen komputasi stateless dalam infrastruktur DePIN modular dan mengikuti alur kerja OCCL tingkat tinggi seperti yang diilustrasikan pada Gambar 4.6 di bawah.



Gambar 4.6: Alur Kerja Tingkat Tinggi dari Lapisan Komputasi Off-Chain

1. Node koordinator di lapisan komputasi off-chain mengambil data dari lapisan ketersediaan data berdasarkan konfigurasi proyek DePIN;
2. Node koordinator mengumpulkan data ke node pembuktian yang menganggur atau kumpulan yang dipilih node menganggur di lapisan komputasi off-chain;
3. Node pembuktian melakukan perhitungan yang ditentukan oleh proyek DePIN dan menghasilkan hasil perhitungan dan bukti validitas yang sesuai;
4. Hasil perhitungan dan bukti keabsahan dikembalikan kepada koordinator simpul;
5. Node koordinator mengirimkan hasil komputasi dan bukti validitas ke kontrak pintar untuk diproses lebih lanjut.

Setelah bukti berhasil diverifikasi secara on-chain, hasil komputasi dapat dipercaya dan digunakan oleh dApp proyek DePIN.

4.3 Verifikasi DePIN dan AI Off-Chain

Rangkaian pembukti komprehensif yang tersedia di W3bstream memungkinkan pengembang membuktikan integritas komputasi off-chain ke blockchain lapisan-1 untuk

berbagai aplikasi DePIN. Secara khusus, pengembang dapat memilih teknik komputasi terverifikasi yang paling sesuai untuk aplikasi tertentu.

4.3.1 Verifikasi DePIN

Seperti yang ditunjukkan oleh Guy Woullet dari a16z [43], keberhasilan DePIN bergantung pada penyelesaian tantangan penting: memastikan verifikasi tepercaya atas node layanan yang tersebar secara geografis tanpa memerlukan otoritas pusat. Teknologi verifikasi DePIN saat ini secara kasar dapat diklasifikasikan menjadi tiga kategori [44], yaitu pendekatan berbasis perangkat keras tepercaya, pendekatan statistik, dan pendekatan berbasis bukti validitas. Setiap pendekatan verifikasi mempunyai kelebihan dan kekurangannya masing-masing dan kombinasi beberapa pendekatan mungkin diperlukan dalam praktiknya. W3bstream memfasilitasi berbagai proyek DePIN untuk diterapkan dan kemudian memperbarui algoritma verifikasinya di platform. Algoritme verifikasi ini dapat ditulis dalam bahasa pemrograman tingkat tinggi seperti Rust, Golang, C++, dll. Dengan menggunakan salah satu prover yang disediakan di W3bstream, keandalan algoritma verifikasi DePIN dapat dijamin.

4.3.2 AI Luar Rantai

Aplikasi DePIN membuka peluang baru untuk pelatihan dan inferensi AI di berbagai sektor industri. Di satu sisi, aplikasi DePIN mampu membawa data dunia nyata dalam jumlah besar ke Web3 dengan cara yang dapat dipercaya, sehingga dapat meningkatkan akurasi model AI secara signifikan. Di sisi lain, aplikasi DePIN dapat secara efektif mengatur sumber daya komputasi dan penyimpanan untuk pelatihan dan inferensi AI dalam skala global. Namun, aplikasi AI sering kali memerlukan komputasi yang intensif dan menimbulkan tantangan yang signifikan untuk diterapkan secara on-chain. W3bstream memungkinkan pengembang untuk melakukan komputasi AI off-chain dan memastikan proses komputasi dapat dipercaya secara bersamaan. Meskipun bukti tanpa pengetahuan mampu memberikan perlindungan integrasi yang kuat untuk komputasi off-chain, penerapan bukti tanpa pengetahuan untuk AI (misalnya, ZKML) mungkin dengan mudah menimbulkan overhead 10.000x hingga 100.000x jika dibandingkan dengan komputasi AI yang tidak dapat diverifikasi [45]. Sebagai pengganti penggunaan

pembuktian ZKP, pengembang dapat beralih ke pembuktian TEE yang lebih efisien untuk komputasi AI off-chain di W3bstream. Pekerjaan awal kami [7, 8] yang dibangun berdasarkan kerangka kerja Arm's Veracruz dan Nitro enclave AWS

Bab 5

ioID - Sistem Identitas Terpadu untuk DePIN

Aplikasi DePIN melibatkan interaksi on-chain (yaitu, staking, transfer aset, peminjaman, dll.) dan off-chain (yaitu, orang-ke-mesin dan mesin-ke-mesin) yang ekstensif di antara peserta sistem yang berbeda. Lapisan identitas dalam infrastruktur DePIN modular merupakan komponen penting untuk mengelola hubungan berbagai entitas dan memastikan interaksi yang aman di antara mereka. Oleh karena itu, merancang lapisan identitas terpadu yang mampu memenuhi persyaratan interaksi on-chain dan off-chain sangat diinginkan untuk aplikasi DePIN.

5.1 Identitas On-Chain vs. Off-Chain

5.1.1 Identitas Dalam Rantai

Tujuan utama dari identitas on-chain adalah untuk membuktikan kepemilikan aset kripto dan melakukan berbagai operasi terkait aset kripto seperti transfer, staking, peminjaman, dll. Alamat blockchain dari Akun Milik Eksternal (EOA) atau Kontrak Cerdas Wallet (SCW) sebagaimana ditentukan dalam ERC-4337 [25] berfungsi dengan baik untuk tujuan ini. Secara khusus, SCW yang memungkinkan logika verifikasi sewenang-wenang mampu mengabstraksi kompleksitas transaksi blockchain (misalnya, verifikasi tanda tangan, kenaikan nonce, pembayaran gas, kompatibilitas rantai, dll.) dan membuat interaksi dengan blockchain menjadi lebih intuitif bagi pengguna akhir. Atribut tambahan (misalnya, partisipasi acara, pemungutan suara proposal, dll.) juga dapat dikaitkan dengan identitas on-chain (yaitu, alamat blockchain) melalui Non-Fungible

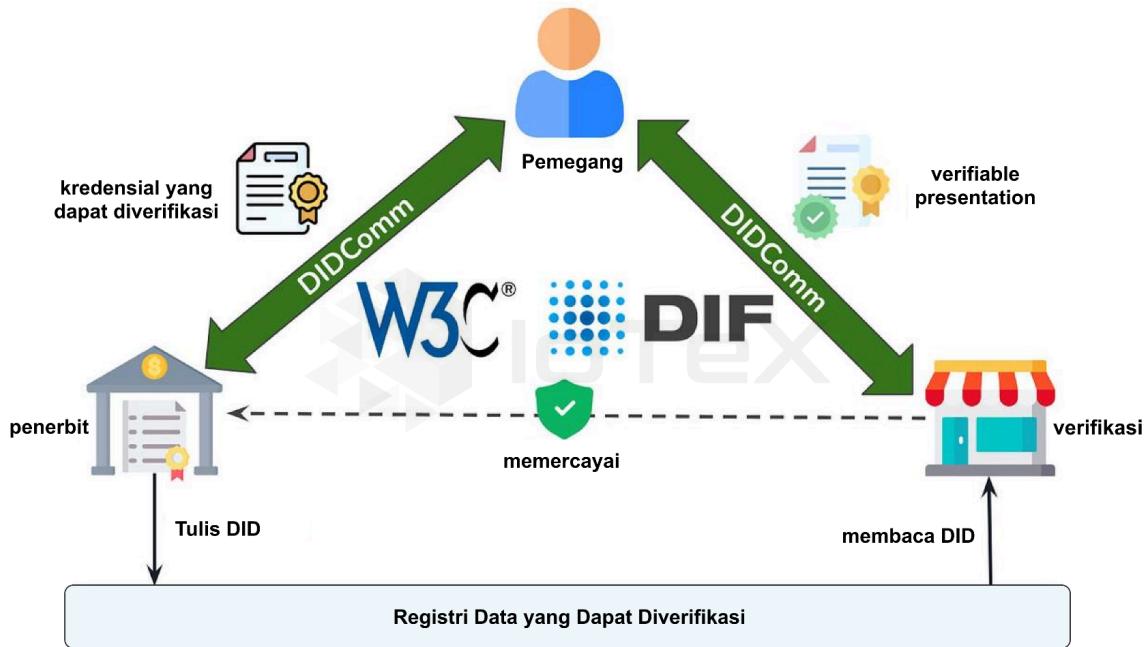
Tokens (NFTs) [26] atau Soulbound Tokens (SBTs) [27]. Atribut tersebut mungkin diperlukan untuk dApps tertentu (misalnya, token airdrop).

5.1.2 Identitas Luar Rantai

Dalam aplikasi DePIN, identitas off-chain diperlukan untuk membangun hubungan orang-ke-mesin dan mesin-ke-mesin yang tepercaya. Sementara sertifikat digital (misalnya, X.509), yang mengikat identitas ke kunci publik, banyak digunakan untuk memungkinkan kepercayaan dalam sistem terpusat, identitas kedaulatan diri (SSI) [48] memberikan solusi identitas yang menjanjikan untuk mengamankan komunikasi antara dua entitas dalam lingkungan yang terdesentralisasi. Seperti yang diilustrasikan pada Gambar 5.1, SSI terdiri dari tiga pilar utama, yaitu pengidentifikasi terdesentralisasi (DID) [49], kredensial yang dapat diverifikasi (VC) [51] dan pesan DIDComm [50]. Setelah setiap peserta (yaitu, orang atau mesin) dalam sistem terdesentralisasi mendaftarkan DID-nya pada registri data yang dapat diverifikasi (misalnya, blockchain), dua entitas dapat membangun saluran komunikasi yang aman dan mengautentikasi satu sama lain dengan bertukar pesan DIDComm. VC berguna ketika atribut identitas tambahan diperlukan untuk dibuktikan oleh entitas tertentu (misalnya, penerbit VC).

5.2 Desain ioID

ioID, yang memanfaatkan alamat dompet blockchain (baik dompet Akun Milik Eksternal (EOA) atau Abstraksi Akun (AA)) sebagai identitas on-chain dan DID sebagai identitas off-chain, adalah sistem identitas terpadu yang dirancang oleh IoTeX untuk penanganan hubungan digital on-chain dan off-chain antara peserta dalam aplikasi DePIN. Sebagai sistem identitas tujuan umum, kami membayangkan ioID bisa melakukannya

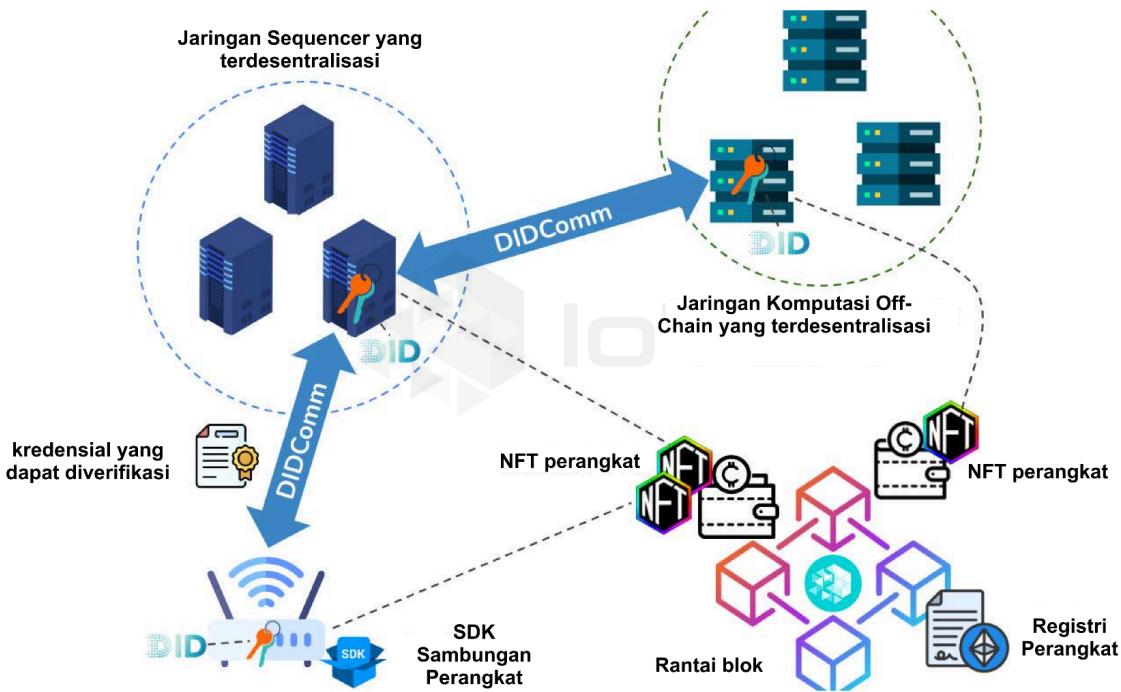


Gambar 5.1: Tiga Pilar Utama SSI

digunakan di berbagai lapisan infrastruktur modular DePIN, seperti yang ditunjukkan pada Gambar 5.2.

5.2.1 Pembuatan ioID pada Perangkat

Perangkat DePIN dapat menghasilkan DID dan dokumen DID yang sesuai dengan cepat di dalam perangkat dengan mengintegrasikan ioConnect SDK IoTeX [16]. Untuk node DePIN yang dikerahkan untuk mendukung pengoperasian lapisan terpusat atau terdesentralisasi tertentu dalam tumpukan DePIN modular, operator node dapat menghasilkan dokumen DID dan DID menggunakan antarmuka baris perintah (CLI). Untuk perangkat DePIN tertanam, produsen dapat mengintegrasikan SDK ioConnect ke dalam firmware perangkat dan memungkinkan pengguna membaca dokumen DID dan DID (misalnya, melalui port serial) dari perangkat.

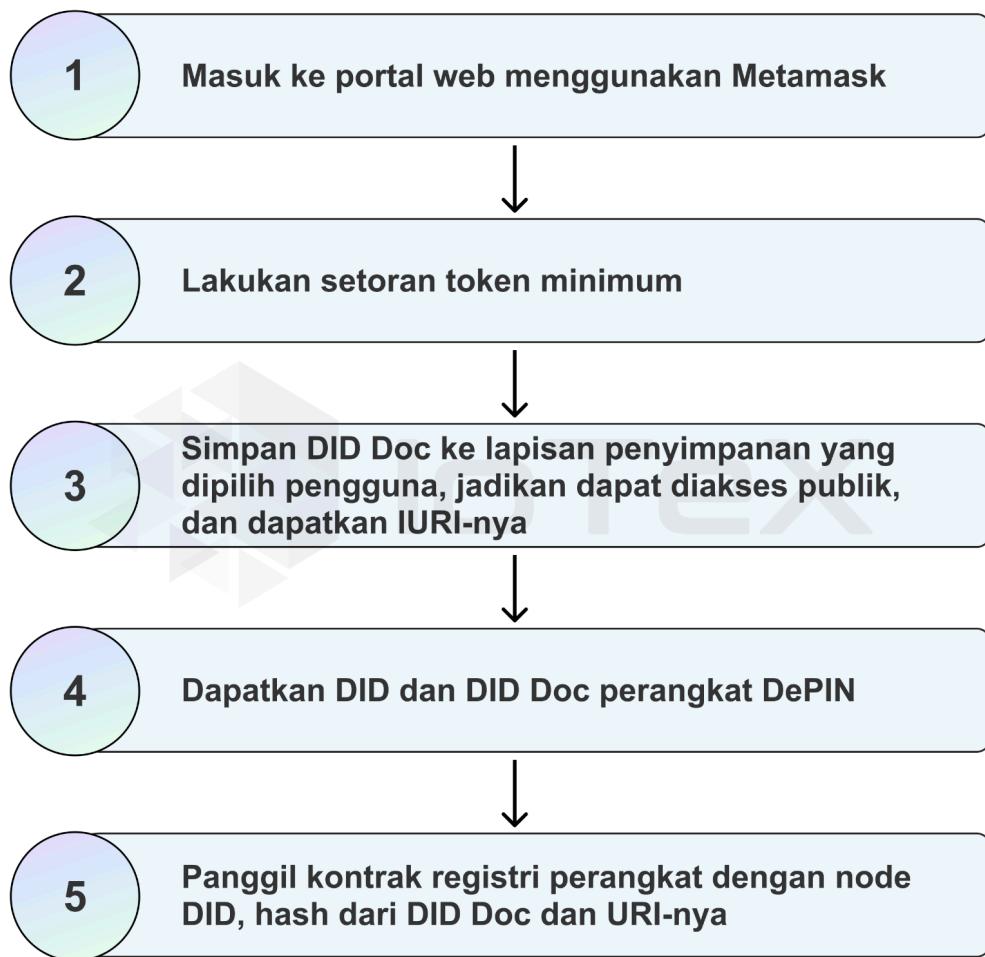


Gambar 5.2: Gambaran Umum Sistem Identitas ioID

5.2.2 Pembuatan ioID pada Perangkat

Pemilik perangkat DePIN dapat melakukan onboarding perangkat melalui portal web (misalnya, Portal MachineFi IoTeX). Proses orientasi ditunjukkan pada Gambar 5.3.

1. Pemilik perangkat pertama kali masuk ke portal web menggunakan Metamask;
2. Pemilik perangkat melakukan deposit token minimum (misalnya 10 token IOTX) di portal web. Token tersebut digunakan untuk membayar biaya bahan bakar selama proses orientasi perangkat;
3. Pemilik perangkat mendapatkan DID dan Dokumen DID perangkat DePIN:
 - a) Untuk node DePIN, pemilik perangkat (yaitu operator node) perlu masuk ke node secara lokal atau jarak jauh dan menggunakan CLI untuk menghasilkan DID dan Dokumen DID yang sesuai pada node;
 - b) Untuk perangkat DePIN yang tertanam, pemilik perangkat harus melakukannya
 - i. Hubungkan perangkat ke PC melalui USB;



Gambar 5.3: Perjalan Penambang untuk Melakukan Orientasi Perangkat DePIN

- ii. Klik tombol "Baca Perangkat DID & DID Doc" di portal web untuk mengambil DID perangkat dan DID Doc melalui port serial;
4. Pemilik perangkat memilih penyedia lapisan penyimpanan terpusat atau terdesentralisasi (misalnya, AWS S3, IPFS, dll.), menyimpan Dokumen DID, membuatnya dapat diakses publik, dan mendapatkan URI-nya;
5. Pemilik perangkat meminta kontrak registri perangkat dengan perangkat tersebut DID, hash dari Dokumen DID, dan URI dari Dokumen DID.

Setelah proses orientasi perangkat berhasil, pemilik perangkat DePIN dapat melihat NFT perangkat ditampilkan di dompet blockchain miliknya, yang mewakili kepemilikan on-chain atas perangkat DePIN.

5.2.3 Mengamankan Interaksi Mesin-ke-Mesin

Setelah DID perangkat DePIN didaftarkan secara on-chain selama proses onboarding perangkat, DID tersebut dapat melakukan komunikasi off-chain yang aman dengan entitas lain di jaringan berdasarkan protokol pesan DIDComm standar.

5.3 Integrasi ioID dalam Proyek DePIN

Proyek DePIN perlu menyelesaikan sejumlah pengaturan sebelum menggunakan modul ioID.

5.3.1 Kontrak Cerdas di ioID

Rangkaian kontrak pintar ioID memberikan kerangka kerja yang kuat untuk manajemen identitas terdesentralisasi pada blockchain IoTeX. Kontrak ini secara kolektif memberikan kerangka kerja yang kuat untuk manajemen identitas dan interaksi dalam ekosistem IoTeX.

- **Registri Proyek DePIN:** Registri Proyek DePIN adalah registri ulang berbasis NFT yang mengelola semua proyek DePIN. Ini memastikan bahwa setiap proyek diidentifikasi dan diautentikasi secara unik dalam jaringan.
- **Kontrak ioID NFT:** Kontrak ioID NFT adalah bagian penting dari kerangka kerja ioID untuk manajemen identitas terdesentralisasi pada blockchain IoTeX. Ini dikelola langsung oleh Project Registry dan bertanggung jawab untuk membuat dan menetapkan token ioID unik untuk perangkat. Ini melibatkan menghubungkan perangkat ke ID proyek dan pemilik, dan menghasilkan alamat dompet terkait sesuai dengan standar ERC6551.

- **ioID Store:** ioID Store bertanggung jawab untuk mengelola aplikasi dan aktivasi ioID di seluruh proyek. Ini menangani siklus hidup aplikasi manajemen identitas, memastikan bahwa identitas diatur dan dipelihara dengan benar
- **ioID Registry:** Kontrak ioID Registry digunakan untuk mendaftarkan perangkat secara on-chain dan mengaktifkan ioID-nya. Ini juga berfungsi sebagai penyelesai DID, menyediakan sarana yang andal untuk memverifikasi identitas perangkat di berbagai proyek.

5.3.2 Menyebarkan Kontrak NFT Perangkat

Untuk mengintegrasikan proyek DePIN dengan modul IoTeX ioID, pemilik proyek memulai dengan menerapkan kontrak "Perangkat NFT" untuk memberi token pada setiap perangkat dalam proyek mereka. Pengguna yang memiliki perangkat NFT dari proyek DePIN berhak mendaftarkan identitas ioID baru untuk perangkat fisik dan mengikatnya ke dompet blockchain mereka. Saat ioID baru didaftarkan untuk suatu perangkat, ioID NFT dicetak ke dompet pemilik, dan NFT perangkat terkait ditransfer ke dompet ERC-6551 di ioID. Proses ini secara efektif "mengaktifkan" ioID, menghubungkan perangkat fisik dengan identitas digitalnya dan dengan pemiliknya di blockchain.

5.3.3 Mendaftarkan Proyek DePIN

Setiap proyek DePIN yang ingin menggunakan identitas ioID harus mengajukan sejumlah ioID dengan membayar jumlah yang diperlukan. ioID hanya dapat diminta oleh proyek DePIN yang terdaftar di blockchain IoTeX. Pemilik proyek dapat melakukan panggilan kontrak pintar langsung atau menggunakan antarmuka baris perintah IoTeX (yaitu, ioclt) untuk mendaftarkan proyek DePIN. Setelah transaksi selesai, Anda akan menerima Proyek NFT dengan ID Token tertentu, yang mewakili ID Proyek DePIN Anda di blockchain IoTeX.

5.3.4 Mengatur Kontrak NFT Perangkat

Setelah mendaftarkan proyek DePIN, langkah selanjutnya adalah mengatur kontrak NFT Perangkat untuk proyek tersebut di ioID Store. Kontrak ini harus ditetapkan sebelum perangkat mencoba mendaftarkan ioID untuk proyek Anda. Pemilik proyek dapat melakukan panggilan kontrak pintar langsung atau menggunakan antarmuka baris perintah IoTeX (yaitu, ioctl) untuk menyelesaikan langkah ini.

5.3.5 Meminta ioID

Pemilik proyek perlu mengajukan ioID dengan membayar jumlah token IOTX yang diperlukan. Jumlahnya ditentukan oleh jumlah ioID yang diminta. Pemilik proyek dapat melakukan panggilan kontrak pintar langsung atau menggunakan perintah IoTeX antarmuka baris (yaitu, ioctl) untuk meminta ioID. Setelah transaksi, jumlah ioID yang diminta akan dikaitkan dengan proyek DePIN.

5.3.6 Mendaftarkan Perangkat

Setelah mengatur kontrak NFT Perangkat dan meminta sejumlah ioID untuk proyek DePIN, perangkat fisik sekarang dapat diaktifkan untuk proyek tersebut dengan mendaftarkannya dalam kontrak ioIDRegistry. Proses ini dilakukan oleh pemilik perangkat dan akan mencetak ioID NFT baru ke akun pemilik perangkat, mengikatnya ke DID perangkat dan ke NFT Perangkat.

Bab 6

ioConnect - SDK Tertanam Universal untuk Memberdayakan Abstraksi Perangkat

Aplikasi DePIN melibatkan perangkat keras yang terdiversifikasi dengan kemampuan dan fungsi berbeda. Tujuan utama dari Lapisan Abstraksi Perangkat Keras (HAL) dalam infrastruktur modular DePIN adalah untuk mengabstraksi kompleksitas dan heterogenitas berbagai perangkat pintar (besar atau kecil) dan memfasilitasi mereka untuk terhubung dengan Lapisan Konektivitas terpusat atau terdesentralisasi (CL) dengan cara yang aman, seperti diilustrasikan pada Gambar 6.1. Pertanyaan yang menantang adalah merancang SDK tertanam universal yang memungkinkan produsen perangkat menghubungkan perangkat mereka ke backend DePIN dengan mudah. Dalam praktiknya, ioConnect SDK bertujuan untuk mendukung keluarga mikrokontroler populer (misalnya, ESP32, Arduino, STM32, dll.), komputer papan tunggal (misalnya, Raspberry Pi, ODROID, Rock Pi, dll.), dan ponsel pintar (misalnya, Android dan iOS) sangat diinginkan.



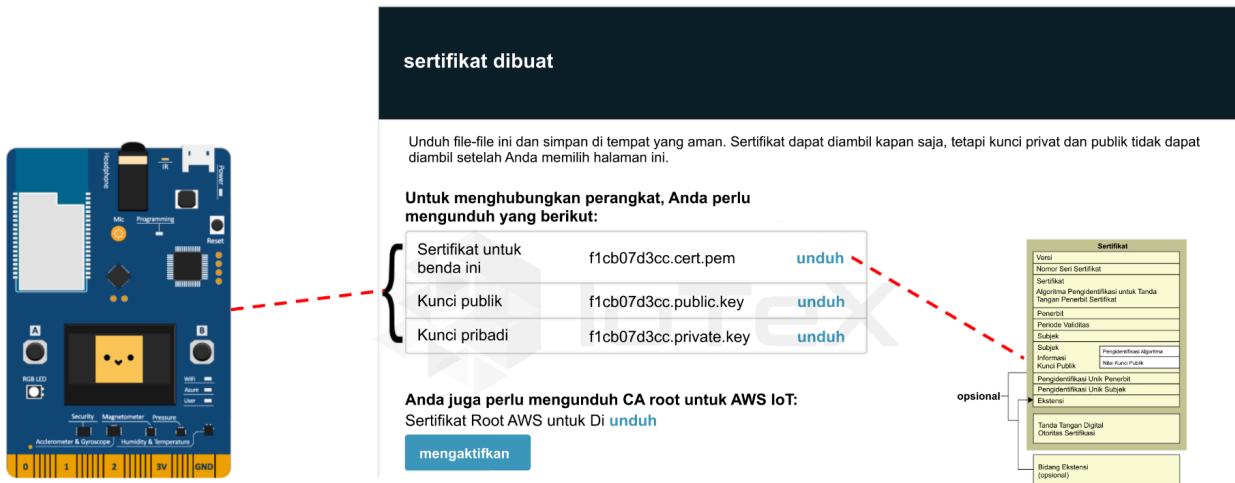
Gambar 6.1: Koneksi Aman antara HAL dan CL

6.1 Pilihan Konektivitas

6.1.1 Menghubungkan ke Lapisan Konektivitas Terpusat

Menghubungkan perangkat pintar ke lapisan konektivitas terpusat (misalnya gateway IoT berbasis cloud) telah diselidiki secara luas di industri IoT tradisional dan diadopsi oleh beberapa proyek DePIN tahap awal karena kematangan teknologinya. Sertifikat digital (misalnya X.509) sering digunakan untuk memastikan komunikasi yang aman antara perangkat pintar dan lapisan konektivitas terpusat. Dengan menggunakan gateway IoT berbasis cloud (misalnya, AWS IoT Core [46]) sebagai contoh (lihat Gambar 6.2), pengguna dapat terlebih dahulu membuat kembaran digital di cloud dan menghasilkan sertifikat perangkat. Setelah sertifikat dipasang di perangkat pintar, sertifikat tersebut dapat membuat koneksi TLS yang aman dengan gateway IoT berbasis cloud. Kembaran digital kemudian berinteraksi dengan layanan lain di cloud atas nama perangkat pintar.

Lapisan konektivitas terpusat, meskipun menyederhanakan koneksi dan pengelolaan perangkat, mewakili satu titik kegagalan dalam aplikasi DePIN dan penerapan lapisan konektivitas terdesentralisasi harus dipertimbangkan secara serius oleh



Gambar 6.2: Onboarding Perangkat dengan AWS IoT Core

proyek DePIN di masa depan.

6.1.2 Menghubungkan ke Lapisan Konektivitas Terdesentralisasi

Meskipun lapisan konektivitas terdesentralisasi menawarkan koneksi jaringan yang lebih kuat untuk aplikasi DePIN, menghubungkan perangkat pintar ke lapisan tersebut menimbulkan sejumlah tantangan teknis:

- Bagaimana perangkat pintar dapat terhubung secara aman dengan node di lapisan konektivitas terdesentralisasi tanpa bergantung pada otoritas sertifikat (CA) terpusat dan sertifikat digital?
- Bagaimana perangkat pintar bisa saling mengautentikasi dengan node di lapisan konektivitas terdesentralisasi?

- Bagaimana perangkat pintar membangun saluran aman dengan node di de-lapisan konektivitas terpusat?

Untuk mengatasi tantangan teknis yang disebutkan di atas, perangkat DePIN harus mewujudkan teknologi dan protokol baru yang dapat digunakan dalam lingkungan yang terdesentralisasi.

6.2 Pertimbangan Desain untuk Membangun SDK Tertanam Universal untuk Perangkat DePIN

Potensi tantangan dalam menghubungkan berbagai perangkat pintar ke lapisan konektivitas terdesentralisasi telah menyebabkan persyaratan desain berikut untuk mengembangkan SDK tertanam universal untuk perangkat DePIN:

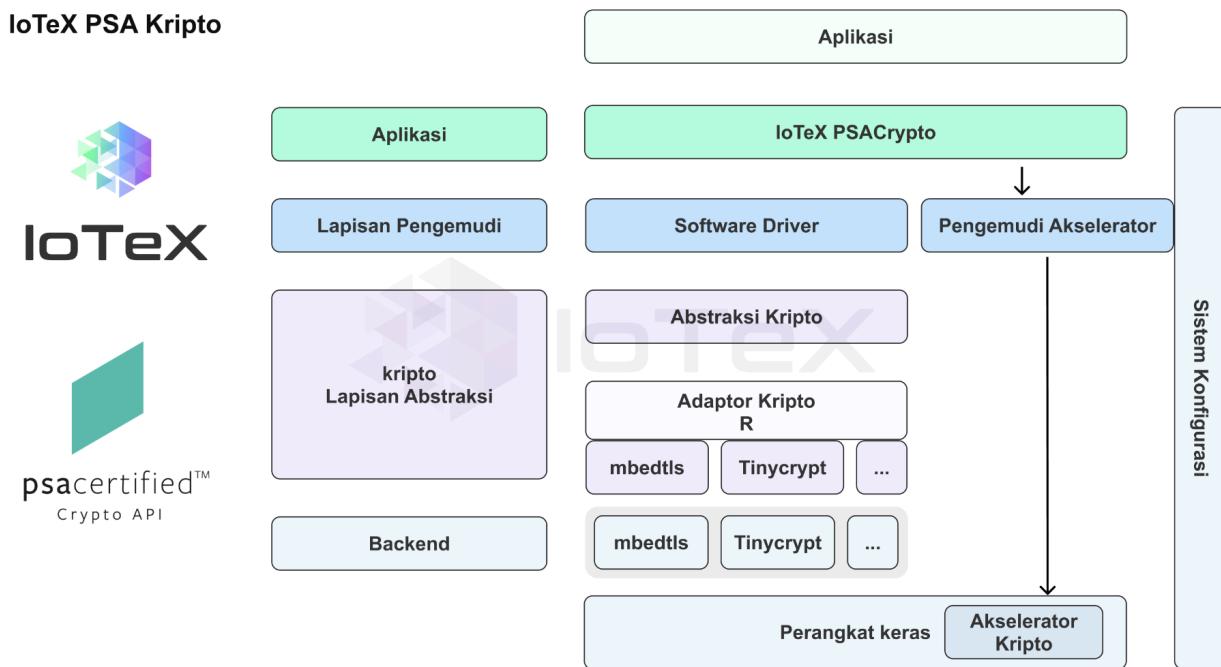
- SDK harus mengakomodasi chipset dan platform perangkat keras yang populer (misalnya mikrokontroler, komputer papan tunggal, telepon pintar, dll.);
- SDK harus mudah diintegrasikan oleh produsen perangkat DePIN perangkat mereka;
- SDK harus mengizinkan perangkat DePIN menggunakan fungsi keamanan tingkat lanjut- ities (misalnya, elemen aman, akselerator kriptografi, dll.);
- SDK harus memungkinkan perangkat DePIN untuk membangun hubungan tepercaya dengan entitas lain (misalnya manusia atau mesin) dalam lingkungan yang terdesentralisasi.

Persyaratan desain tersebut telah memotivasi kami untuk mengeksplorasi teknologi baru seperti API kripto bersertifikasi PSA Arm dan identitas kedaulatan diri (SSI) serta metodologi desain SDK berlapis.

6.2.1 API Kripto Bersertifikat PSA Arm

API kripto bersertifikasi PSA Arm [47] mendefinisikan antarmuka standar dan terpadu untuk mengakses operasi kriptografi dan layanan manajemen kunci pada berbagai platform perangkat keras. Dengan memuat driver perangkat lunak/perangkat keras

kriptografi yang tersedia pada platform perangkat keras target, pengembang dapat dengan mudah mengakses semua fungsi terkait keamanan melalui API kripto PSA, seperti yang ditunjukkan pada Gambar 6.3.

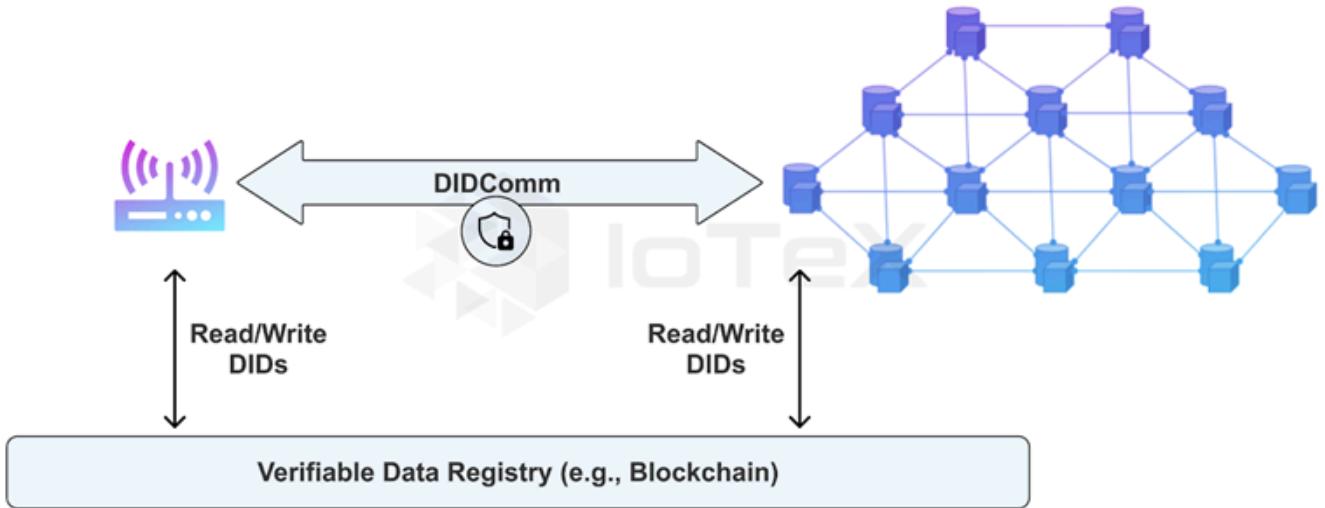


Gambar 6.3: Penggunaan Library PSACrypto IoTeX di Perangkat DePIN

Integrasi API kripto bersertifikasi PSA Arm ke dalam perangkat DePIN dapat membantu berpotensi meningkatkan keamanan perangkat DePIN, sehingga mengurangi peningkatan risiko penipuan dalam aplikasi DePIN secara efektif.

6.2.2 Identitas Kedaulatan Diri (SSI)

Teknik identitas kedaulatan diri (SSI) [48], seperti Pengidentifikasi Terdesentralisasi (DID) [49], Kredensial yang Dapat Diverifikasi (VC) [51] dan pesan DIDComm [50], memindahkan kendali identitas digital dari penyedia identitas konvensional ke penyedia identitas individu. dan meletakkan dasar bagi orang-orang, organisasi, dan hal-hal yang membentuk hubungan digital yang kaya. Dalam lingkungan yang terdesentralisasi, SSI memberikan solusi yang menjanjikan untuk membangun hubungan orang-ke-mesin dan mesin-ke-mesin yang terpercaya tanpa bergantung pada penyedia identitas pihak ketiga yang tersentralisasi atau terfederasi, seperti yang diilustrasikan pada Gambar 6.4.



Gambar 6.4: Komunikasi Berbasis SSI dalam Lingkungan Terdesentralisasi

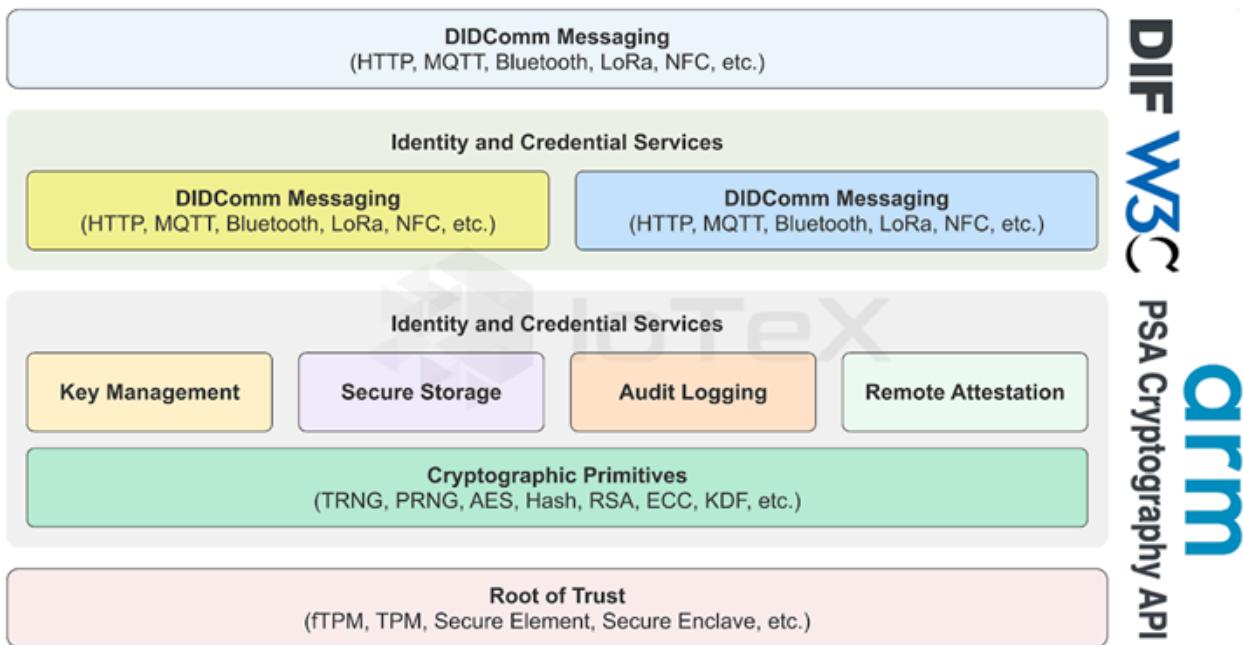
6.3 Spesifikasi Implementasi

ioConnect [16] adalah SDK tertanam universal yang dirancang khusus oleh IoTeX untuk memberdayakan perangkat DePIN. Untuk mendukung berbagai perangkat pintar dan persyaratan aplikasi, SDK dirancang dengan inti SDK dan lapisan adaptasi platform (PAL).

6.3.1 Inti SDK ioConnect

Inti dari ioConnect terdiri dari empat lapisan seperti yang ditunjukkan pada Gambar 6.5. Dua lapisan terbawah mewujudkan spesifikasi API kripto bersertifikasi PSA Arm v1.1, sedangkan dua lapisan teratas menerapkan tiga pilar utama (yaitu, DID, VC, dan DIDComm) di SSI. Semua operasi kriptografi yang diperlukan dalam SSI dilakukan melalui panggilan API kripto PSA.

Perhatikan bahwa inti SDK ioConnect tidak bergantung pada platform perangkat keras dan tidak terikat pada komponen/sumber daya tertentu pada perangkat DePIN.

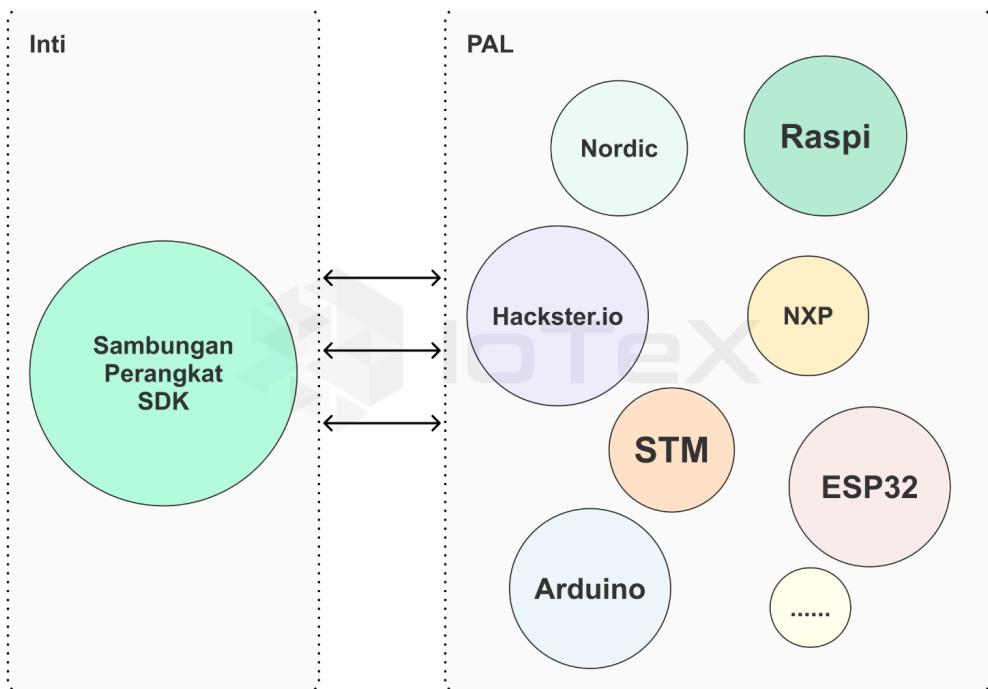


Gambar 6.5: Inti SDK ioConnect

6.3.2 Kompatibilitas Perangkat DePIN

Untuk mengakomodasi berbagai perangkat DePIN, seluruh SDK ioConnect mengadopsi metodologi desain berlapis seperti yang diilustrasikan pada Gambar 6.6. Di tangan satunya, Core berisi implementasi spesifikasi perangkat keras yang independen (misalnya, SSI, API kripto PSA, dll.), yang ditangani oleh Lapisan Adaptasi Platform (PAL). perbedaan antara berbagai sistem dan platform tertanam (misalnya, aturan kompilasi, konvensi pengkodean, desain kerangka kerja, dll.).

Pengenalan PAL memungkinkan pengembang dengan mudah menambahkan dukungan perangkat keras baru dengan hanya mengembangkan komponen PAL lain dengan hanya 300 hingga 500 baris kode, sehingga secara efektif mengatasi masalah kompatibilitas perangkat DePIN dan secara



Gambar 6.6: Arsitektur Berlapis di ioConnect SDK

Bab 7

ioDDK - Mengaktifkan Rantai Aplikasi DePIN yang Berdaulat Sendiri

7.1 Alasan Desain

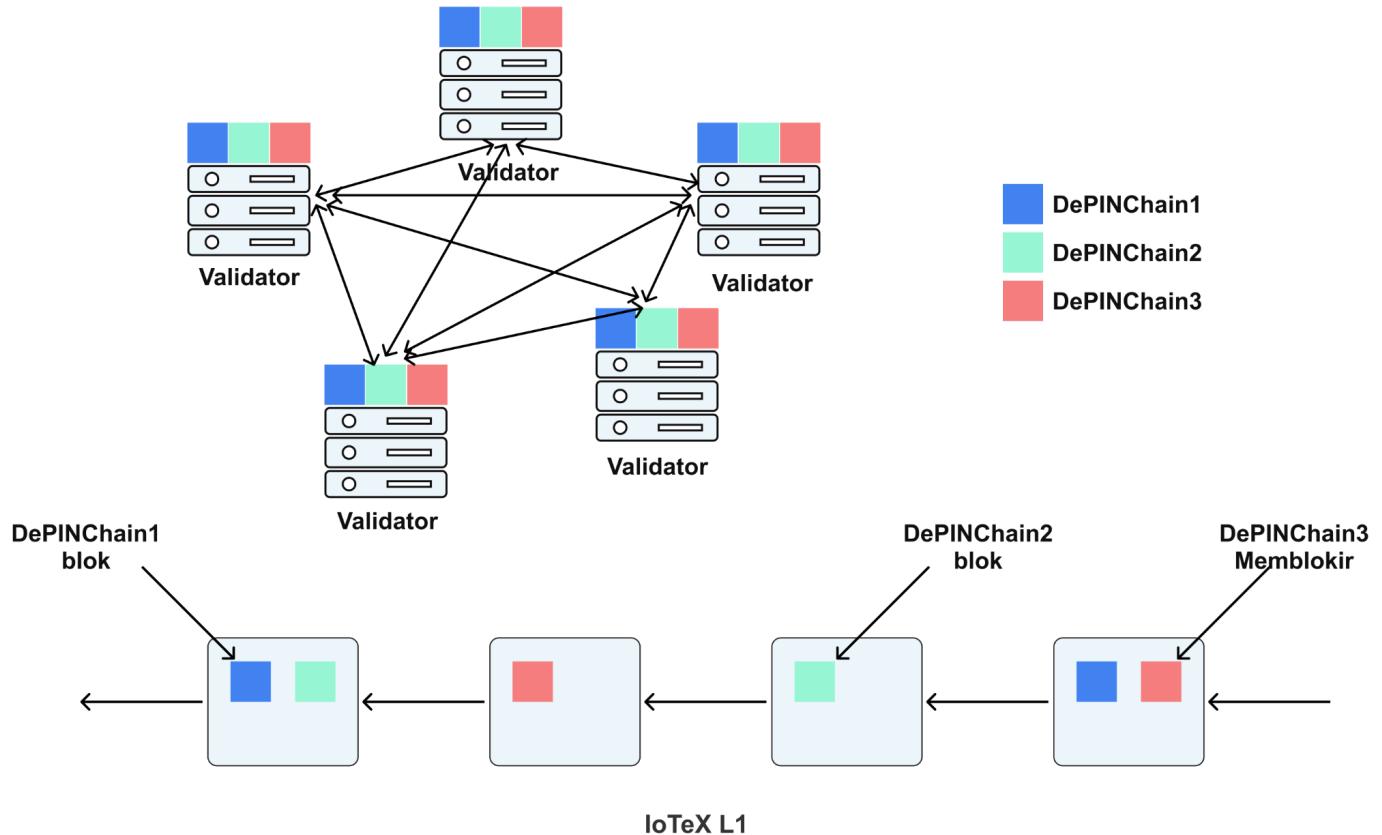
Alasan di balik mengaktifkan L2 khusus aplikasi untuk proyek DePIN di IoTeX L1 didorong oleh beberapa faktor yang mendorong.

- Pertama, L2 khusus aplikasi sangat penting untuk proyek DePIN karena L2 tersebut memungkinkan pengenalan tokenomik unik, pengalaman pengguna yang disesuaikan (misalnya, dompet dan browser), dan struktur tata kelola yang disesuaikan. Kustomisasi ini sangat penting untuk mengoptimalkan blockchain guna memenuhi kebutuhan spesifik dan skenario setiap aplikasi DePIN pada skalabilitas, memastikan bahwa masing-masing proyek dapat mencapai potensi penuhnya.
- Selain itu, banyak proyek DePIN yang kekurangan keahlian dan sumber daya keuangan diharuskan untuk membangun dan memelihara infrastruktur blockchain mereka sendiri.

Saat ini, IoTeX L1 diamankan oleh kumpulan 120+ delegasi yang didistribusikan secara global (yaitu, validator) melalui protokol konsensus Randomized Delegated Proof-of-Stake (Roll-DPoS) internal kami [52]. Dengan memanfaatkan ruang blok aman dari IoTeX L1, proyek DEPIN ini dapat meluncurkan L2 khusus aplikasi mereka dengan lancar tanpa beban berat yang terkait dengan pengembangan blockchain.

ioDDK adalah SDK rantai yang memungkinkan proyek DePIN menyediakan rantai aplikasi yang berdaulat sendiri dan mewarisi keamanan IoTeX L1 secara bersamaan, seperti yang diilustrasikan pada Gambar 7.1. Saat memvalidasi dan mengusulkan blok

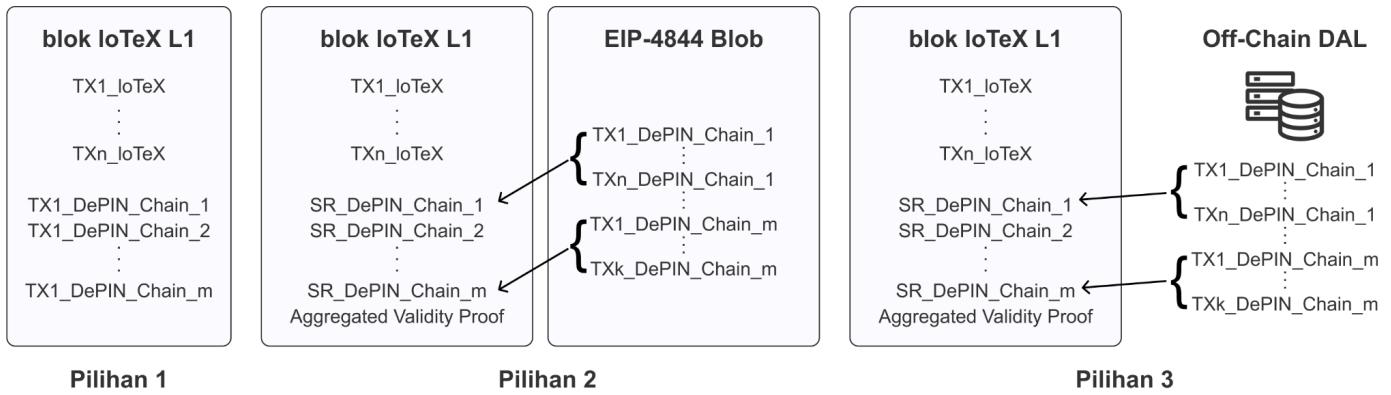
IoTeX L1, validator juga mencapai konsensus mengenai transaksi dari rantai aplikasi DePIN. Dengan menyewakan blockspace, IoTeX L1 dapat memberi proyek DePIN sumber daya yang diperlukan untuk menerapkan solusi khusus mereka secara efisien, tanpa memerlukan investasi awal atau pengetahuan teknis yang signifikan, sehingga mendorong ekosistem yang lebih dinamis dan inovatif.



Gambar 7.1: Rantai Aplikasi DePIN Berdaulat yang Diamankan oleh IoTeX L1

7.2 Blockspace dan Validator Bersama

Untuk meminimalkan kompleksitas pengembangan, semua rantai DePIN yang berdaulat dapat berbagi blockspace dan validator dengan IoTeX L1. Tiga opsi implementasi bisa dipertimbangkan dalam praktiknya, seperti yang diilustrasikan pada Gambar 7.2.



Gambar 7.2: Tiga Opsi Implementasi untuk Shared Blockspace dan Validator

Opsi 1 - Menyimpan Semua Transaksi di IoTeX L1

Dalam opsi ini, transaksi dari rantai DePIN yang berdaulat bersama dengan transaksi di IoTeX L1 berbagi ruang blok yang sama dan semua transaksi harus melalui proses konsensus IoTeX L1. Pendekatan ini memastikan bahwa semua rantai DePIN yang berdaulat mencapai keamanan yang sama seperti IoTeX L1. Namun karena keterbatasan ukuran blok, hanya sejumlah proyek DePIN tertentu yang dapat didukung. Proses tata kelola yang terdesentralisasi mungkin diperlukan untuk menentukan proyek DePIN mana yang memenuhi syarat untuk menggunakan pendekatan ini.

Opsi 2 - Menyimpan Transaksi DePIN Chain menggunakan EIP-4844

Dalam opsi ini, transaksi dari rantai DePIN yang berdaulat sendiri disimpan sementara di IoTeX L1 menggunakan blob EIP-4844. Akar negara bersama dengan bukti validitas gabungan transisi negara dari semua rantai DePIN yang berdaulat berbagi ruang blok yang sama dengan transaksi IoTeX L1. Bukti validitas gabungan diverifikasi pada IoTeX L1 untuk menyelesaikan semua transaksi pada rantai DePIN yang berdaulat sendiri. Pendekatan berbasis rollup seperti itu dapat secara efektif meningkatkan skalabilitas sistem dan memungkinkan semua rantai DePIN yang berdaulat untuk mewarisi keamanan IoTeX L1 secara bersamaan. Perhatikan bahwa salah satu pembuktian di jaringan W3bstream harus digunakan untuk mewujudkan pendekatan ini.

Tabel 7.1: Perbandingan Tiga Opsi Implementasi

	Rantai DePIN Penyimpanan Transaksi	Skalabilitas	W3bstream Membutuhkan	Keamanan
Pilihan 1	blok on-chain	Rendah	TIDAK	Tinggi
Pilihan 2	gumpalan on-chain	Tinggi	Ya	Tinggi
Pilihan 3	DAL di luar rantai	Tinggi	Ya	Rendah /Sedang

Table 7.1: Comparison of Three Implementation Options

Opsi 3 - Menyimpan Transaksi DePIN Chain menggunakan DAL Off-Chain

Dalam opsi ini, rantai DePIN yang berdaulat dapat memilih lapisan ketersediaan data (DAL) di luar rantai untuk menyimpan transaksi mereka. Mirip dengan Opsi 2, negara bagian akar bersama dengan bukti validitas agregat transisi keadaan dari semua rantai DePIN yang berdaulat berbagi ruang blok yang sama dengan transaksi IoTeX L1. Bukti validitas agregat diverifikasi di IoTeX L1 untuk menyelesaikan semua transaksi pada rantai DePIN yang berdaulat sendiri. Namun, akar negara harus berkomitmen ke IoTeX L1 oleh DAL dalam pendekatan ini. Meskipun pendekatan berbasis validum juga dapat meningkatkan skalabilitas sistem, keamanannya bergantung pada hal tersebut implementasi DAL tertentu. Perhatikan bahwa salah satu pembuktian di W3bstream jaringan harus dimanfaatkan untuk mewujudkan pendekatan ini.

Perbandingan Tiga Pilihan

Tabel 7.2 memberikan perbandingan ketiga opsi implementasi di atas dengan sehubungan dengan penyimpanan transaksi rantai DePIN, skalabilitas, persyaratan dan keamanan W3bstream.

7.3 Komponen ioDDK dan Alur Kerja Tingkat Tinggi

7.3.1 Komponen ioDDK

ioDDK, yang memungkinkan proyek DePIN memanfaatkan delegasi yang ada (yaitu validator) dan blockspace di IoTeX L1 untuk menjadi tuan rumah rantai DePIN yang berdaulat sendiri, terdiri dari komponen-komponen berikut:

- **Konfigurasi Rantai:** Komponen konfigurasi rantai memungkinkan pengembang untuk mengonfigurasi parameter spesifik (misalnya, tinggi awal, jenis transaksi, persyaratan ruang blok, dll.) dari rantai DePIN;
- **Penerapan Rantai:** Komponen penerapan rantai memungkinkan pengembang mengelola proses penerapan rantai DePIN di seluruh delegasi IoTeX L1;
- **Chain Explorer:** Komponen penjelajah rantai memungkinkan proyek DePIN serta pihak eksternal memantau status dan metrik utama (yaitu, tinggi blok, TPS, detail transaksi, dll.) dari rantai DePIN;
- **Komandan Rantai:** Komandan rantai adalah alat baris perintah yang menyediakan serangkaian perintah untuk menyederhanakan pengembangan dan pengelolaan rantai DePIN.

7.3.2 Alur Kerja Tingkat Tinggi

Setelah proyek DePIN disetujui untuk menyediakan rantai kedaulatan menggunakan ruang blok bersama dan validator di IoTeX L1 (misalnya, melalui proses tata kelola terdesentralisasi), proyek dapat menggunakan ioDDK sebagai berikut:

- Pengembang menggunakan fungsi "Konfigurasi Rantai" di ioDDK untuk menentukan sejumlah parameter spesifik rantai DePIN:
 - **chainID:** pengidentifikasi rantai dihasilkan secara otomatis untuk mewakili rantai DePIN yang berdaulat sendiri;
 - **Jenis transaksi:** berbagai bidang dalam suatu transaksi;
 - **Nomor transaksi maksimum:** jumlah maksimum transaksi berantai DePIN yang diproses dalam blok IoTeX L1;
 - **Pepatah W3bstream:** pemilihan pembuktian W3bstream.

- Pengembang menyiapkan gambar buruh pelabuhan dari logika pemrosesan transaksi untuk rantai DePIN dan menggunakan fungsi `âChain Deploymentâ` di ioDDK untuk menyebarkan gambar buruh pelabuhan ke semua delegasi IoTeX L1.

Setelah logika pemrosesan transaksi khusus rantai DePIN disebarluaskan ke delegasi IoTeX L1, transaksi rantai DePIN akan diproses sebagaimana mestinya. Pengembang dapat menggunakan `âChain Explorerâ` di ioDDK untuk memeriksa status rantai DePIN yang disediakan. Selain itu, pengembang juga dapat menggunakan `âChain Commanderâ` untuk mengelola rantai DePIN menggunakan sejumlah perintah dukungan.

7.4 Pasar Penyewaan Blockspace

Kami berencana untuk menerapkan pasar blockspace yang memungkinkan pengembang untuk memperdagangkan blockspace yang disesuaikan untuk DePIN L2 spesifik mereka yang dibangun dengan ioDDK. Strategi berorientasi pasar ini memastikan alokasi sumber daya beradaptasi dengan permintaan real-time, sehingga mengoptimalkan efisiensi jaringan secara keseluruhan.

Pengenalan blockspace yang dapat diperdagangkan juga berdampak pada utilitas dan likuiditas token IOTX. Misalnya, pengembang dapat mempertaruhkan atau membakar IOTX untuk mendapatkan sejumlah blockspace tertentu. Pendapatan yang dihasilkan dari transaksi dapat dialokasikan dengan berbagai cara, termasuk mendanai perbendaharaan atau dibakar untuk mengatur pasokan token.

7.5 Implikasi pada IoTeX L1

Pengenalan blockspace bersama ke IoTeX L1 menghadirkan sejumlah fitur yang dirancang untuk memenuhi permintaan proyek DePIN L2 yang terus meningkat:

- **Waktu Blokir dan Finalitas yang Cepat:** Salah satu persyaratan utama DePIN L2 adalah waktu blok yang cepat dengan penyelesaian yang cepat untuk

mengoptimalkan pengalaman pengguna. Saat ini, IoTeX L1 memiliki waktu blok 5 detik. Namun, untuk memenuhi kebutuhan proyek DePIN berkinerja tinggi, kami bertujuan untuk mengurangi waktu blok ini menjadi 2 detik. Pengurangan ini secara signifikan akan meningkatkan daya tanggap dan efisiensi aplikasi L2, memastikan pengalaman yang lebih lancar dan ramah pengguna.

- **Peningkatan Throughput dan Desentralisasi:** Total throughput De-PIN L2 secara inheren dibatasi oleh kekuatan komputer semua validator di Jaringan IoTeX L1. Untuk mengatasi hal ini, penting untuk meningkatkan jumlah validator dan meningkatkan desentralisasi jaringan secara keseluruhan. Dengan memperluas kumpulan validator, IoTeX L1 dapat mendukung transaksi yang lebih tinggi volume dan memberikan keamanan yang lebih kuat. Peningkatan ini juga akan memfasilitasi jaringan yang lebih terdesentralisasi dan tangguh, yang penting untuk dipertahankan kepercayaan dan stabilitas dalam ekosistem yang sedang berkembang.

Untuk memenuhi persyaratan di atas, direncanakan penerapan Pemisahan Pengusul-Pembangun (PBS) [53]. PBS adalah konsep yang awalnya diusulkan oleh para peneliti Ethereum yang dirancang untuk meningkatkan ketahanan sensor dan kinerja jaringan blockchain secara keseluruhan. Ini memisahkan peran pengusul blok dan pembuat blok untuk mengoptimalkan produksi blok dan memastikan keadilan dalam proses validasi.

- **Pengusul Blokir:** Bertanggung jawab untuk mengusulkan blok baru berdasarkan kondisi blockchain dan aturan jaringan saat ini. Mereka mengumpulkan transaksi dan membuat proposal blok yang akan divalidasi oleh jaringan. Peran ini kemungkinan besar akan diisi oleh delegasi konsensus saat ini.
- **Pembangun Blok:** Entitas khusus yang berfokus pada pembangunan blok dengan memilih transaksi paling berharga dari actpool, mengoptimalkan penggunaan ruang blok, dan berpotensi meningkatkan throughput. Mereka menyerahkan blok yang mereka buat kepada pengusul, yang kemudian mengusulkan blok tersebut ke jaringan untuk validasi. Ini akan menjadi peran baru yang diperkenalkan ke jaringan IoTeX L1 dan berdedikasi untuk mengerjakan transaksi paket termasuk dari De-PIN L2s.

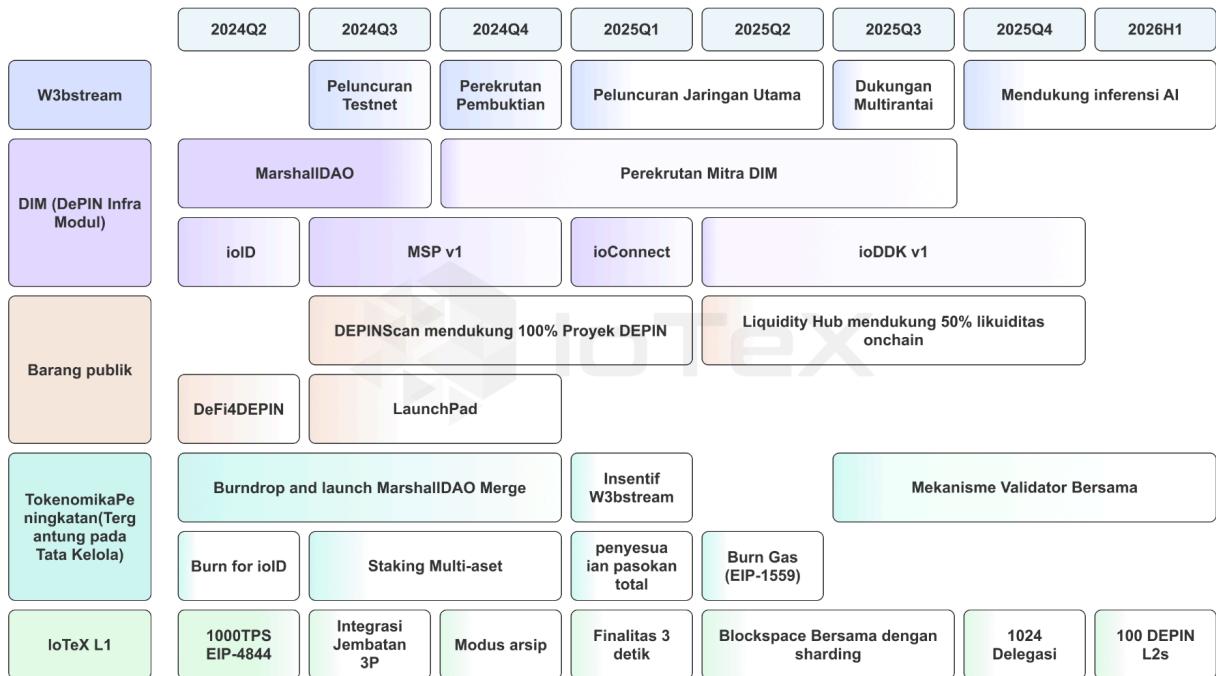
Pemisahan peran-peran ini membantu memitigasi risiko pengendalian dan sensor terpusat dengan mendistribusikan tanggung jawab ke berbagai entitas. Hal ini

meningkatkan kapasitas jaringan dan mengurangi waktu pemrosesan transaksi, yaitu juga memungkinkan produksi blok yang lebih efisien, karena pembangun dapat fokus pada pemilihan transaksi, pengoptimalan, dan bahkan sharding, sementara pengusul menangani proses konsensus dan finalisasi blok. Pendekatan ini akan memastikan bahwa DePIN L2 yang berdasarkan pada blockspace bersama yang disediakan oleh IoTeX L1 dapat beroperasi secara efisien dan aman, memenuhi tuntutan skenario aplikasi spesifiknya.

Bab 8

Peta Jalan Baru

IoTeX 2.0 adalah kumpulan dari berbagai komponen yang kami rencanakan untuk dibangun mulai sekarang hingga tahun 2026. Peta jalannya disajikan di bawah ini pada Gambar 8.1. Perlu diperhatikan bahwa banyak komponen yang terdaftar bergantung pada proposal tata kelola dan pemungutan suara, dan oleh karena itu dapat berubah.



Gambar 8.1: Peta Jalan IoTeX 2.0

Bab 9

Kesimpulan

IoTeX 2.0 menawarkan visi baru untuk Jaringan IoTeX dengan tetap mempertahankan prinsip-prinsip inti yang mendasari dimulainya. Sejak awal, IoTeX telah membayangkan masa depan di mana individu dapat memiliki dan mengontrol perangkat mereka, serta data dan nilai yang dihasilkan perangkat tersebut. IoTeX bertujuan untuk menjadi pusat data dunia nyata dan real-time, yang mendukung jaringan AI super cerdas. Jaringan ini tidak hanya melampaui kecerdasan manusia tetapi juga akan memanfaatkan data yang akurat dan andal yang mencerminkan dunia nyata secara real-time. Pergeseran ini menunjukkan bahwa kebenaran hakiki dan kekuatan pengambilan keputusan akan berakar pada realitas nyata dan dinamis dari lingkungan fisik kita. Transformasi ini mengubah cara data dinilai dan digunakan, sehingga memengaruhi masa depan peradaban. Yang terpenting, semua yang dimungkinkan oleh IoTeX akan dimiliki dan dioperasikan oleh masyarakat, untuk masyarakat.

Terima kasih kepada komunitas IoTeX atas kontribusi, dukungan, dan masukan Anda yang berkelanjutan. Saat kami memulai perjalanan ambisius baru ini, kami tahu bahwa IoTeX dan komunitas global kami akan melakukan perubahan nyata dan menghadirkan DePIN ke setiap negara di dunia. Saatnya membangun!

Penafian

Whitepaper ini merupakan upaya kolaboratif oleh IoTeX coredev dan anggota dari komunitas IoTeX. Ini menguraikan arah yang diusulkan untuk Jaringan IoTeX. Namun, isinya tidak memerlukan komitmen dari penulis atau organisasi masing-masing. Komunitas IoTeX bertanggung jawab untuk mengadaptasi dan mengadopsi langkah-langkah yang diusulkan dalam makalah ini. Keberhasilan setiap proposal pada akhirnya akan bergantung pada kerja keras komunitas luas dan mereka yang membangun Jaringan IoTeX.

Informasi yang disajikan di sini disediakan oleh pihak-pihak yang tercantum di atas (PIHAK) hanya untuk tujuan informasi saja. Baik PARA PIHAK maupun afiliasi, direktur, pejabat, manajer, karyawan, atau perwakilannya tidak membuat pernyataan atau jaminan apa pun, tersurat maupun tersirat, mengenai materi atau informasi apa pun yang terkandung di sini. Selain itu, PIHAK atau individu tersebut tidak memikul atau mempunyai tanggung jawab atau kewajiban apa pun terhadap Anda atau afiliasi Anda, atau masing-masing direktur, pejabat, manajer, karyawan, atau perwakilan afiliasi Anda atau afiliasi Anda yang diakibatkan oleh penggunaan informasi dan materi yang terkandung di dalamnya.

Informasi yang diberikan di sini diberikan dengan itikad baik berdasarkan informasi yang diyakini, namun tidak ada jaminan akurat atau lengkap. Informasi dalam makalah ini tidak boleh dianggap sebagai nasihat investasi, nasihat keuangan, nasihat perdagangan, atau bentuk nasihat lainnya. Disarankan agar Anda melakukan uji tuntas sendiri dan berkonsultasi dengan penasihat keuangan Anda sebelum membuat keputusan investasi apa pun.

Pengakuan

Kami mengucapkan terima kasih yang sebesar-besarnya kepada individu dan perusahaan modal ventura berikut ini (yaitu, Vinayak Kurup dari Escape Velocity (EV3), Robert Koschig dari 1kx, SNZ Capital, Future Money Group (FMG), Álvaro Gracia dari Borderless Capital, Lattice, Summer Capital, Pantera Capital, BlueYard Capital, Spartan Capital, Lemniscap, NGC Ventures, Stanford Blockchain Accelerator, Foresight Venture, dan Samsung NEXT), proyek Web3 (yaitu, NEAR Foundation, RISC0, Helium Foundation, The Graph Foundation, Filecoin Foundation, dan Textile), dan firma riset kripto (yaitu, IntoTheBlock (ITB) dan Messari) yang masukannya yang sangat berharga dan dukungannya yang tak tergoyahkan telah berperan penting dalam penyusunan Whitepaper ini. Keahlian, wawasan, dan komitmen Anda telah meningkatkan kedalaman dan kualitas pekerjaan kami secara signifikan. Kami sangat menghargai waktu dan sumber daya yang telah Anda investasikan, dan kontribusi Anda sangat penting dalam memajukan misi IoTeX 2.0.

Bibliografi

- [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/.](https://www.risczero.com/)
- [29] Succinct Processor 1 (SP1). [https://succinctlabs.github.io/sp1/.](https://succinctlabs.github.io/sp1/)
- [30] Nexus. [https://www.nexus.xyz/.](https://www.nexus.xyz/)
- [31] zkWasm. [https://delphinuslab.com/zk-wasm/.](https://delphinuslab.com/zk-wasm/)
- [32] Circom 2. [https://docs.circom.io/.](https://docs.circom.io/)
- [33] Halo 2. [https://zcash.github.io/halo2/.](https://zcash.github.io/halo2/)
- [34] ZoKrates. [https://zokrates.github.io/.](https://zokrates.github.io/)
- [35] Noir. [https://noir-lang.org/.](https://noir-lang.org/)
- [36] Cairo. [https://www.cairo-lang.org/.](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.](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.](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.](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.](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/.](https://aws.amazon.com/ec2/nitro/)
- [42] Arm Confidential Compute Architecture. [https://www.arm.com/architecture/security-features/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.](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/.](https://iotex.io/blog/decentralized-verification-in-depin/)

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