MOI Lite Paper
Edition April 2023

INTERACTION STATE MACHINES & CONTEXT-AWARE BLOCKCHAIN NETWORKS

Anantha Krishnan – Founder, Sarva Labs Inc
(@ArshaSays)

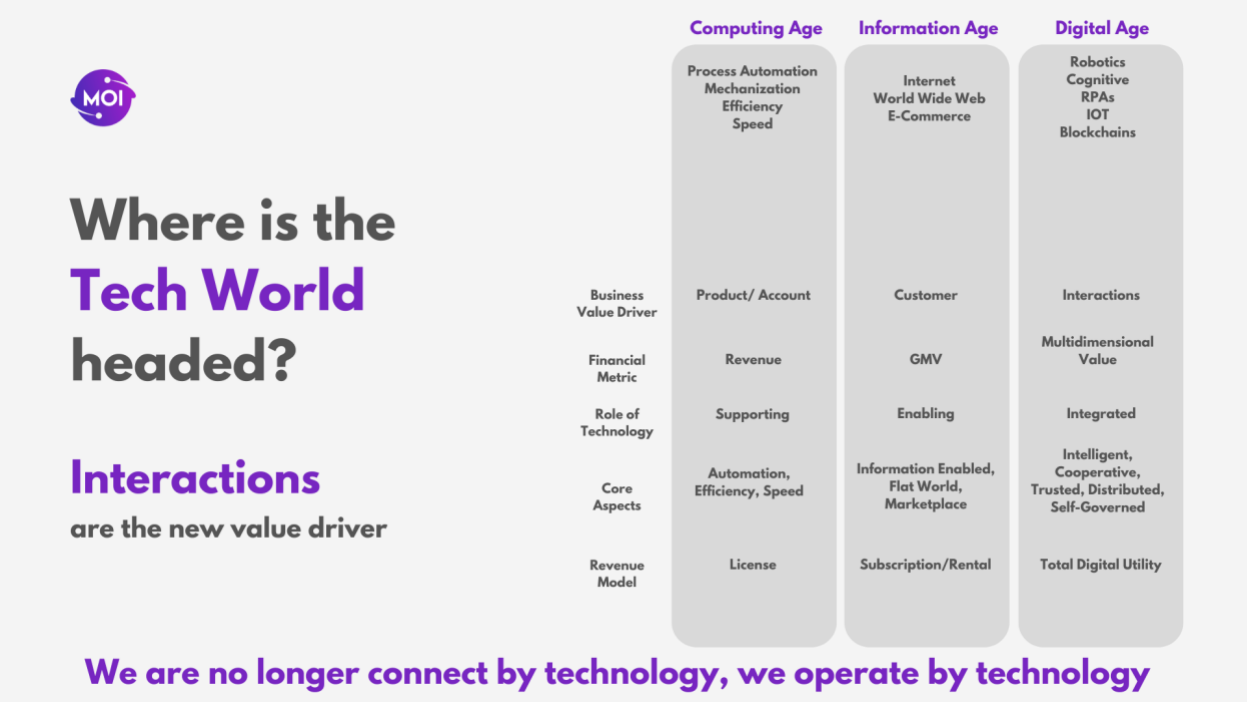
TABLE OF CONTENTS

Today's Challenge

Emergence of the Digital Society & it's needs

The emerging digitally interacting world is evident all around us. We no longer use the internet to simply send emails or search for information. We are beginning to use digital networks to sate the most fundamental of Maslow's hierarchy of needs: learning, eating, socializing, business processes, regulatory governance, money management – all are conducted within a digitally interacting world. More than simply connected by technology, we now operate by technology. This fundamental fact creates new demands on the networks we use.

In this rapidly evolving world, our communication is not limited to just the transfer of information. We are now exchanging diverse values in a more personal and human-like manner. However, transferring values is fundamentally distinct from information transfers, as it requires a high degree of flexibility in terms of value, trust, asset, storage, computing power, and user control based on the specific interaction situation and participant preferences. This necessitates a fully customized user experience for each interaction, which can only be achieved through a stateful decentralized network that is personalized and peer-to-peer.



As the digital society increasingly adopts a fully peer-to-peer and human-like interaction model, the number of multi-dimensional digital assets based on user preferences is growing exponentially, decoupled from apps and currencies. This shift demands significant levels of scalability and flexibility from current smart-contract based blockchain networks. Specifically, the digital world is transitioning from a focus on apps and cryptocurrencies to people, assets, and values. It is moving from a programmatic model to an interactive peer-to-peer model. The number of digital assets is also increasing, with billions of assets defined by the heterogeneous value needs of each participant and their interaction situation, instead of the previous model that relied on thousands of cryptocurrencies. This creates an end-state requirement where the participant is at the center of the interaction.

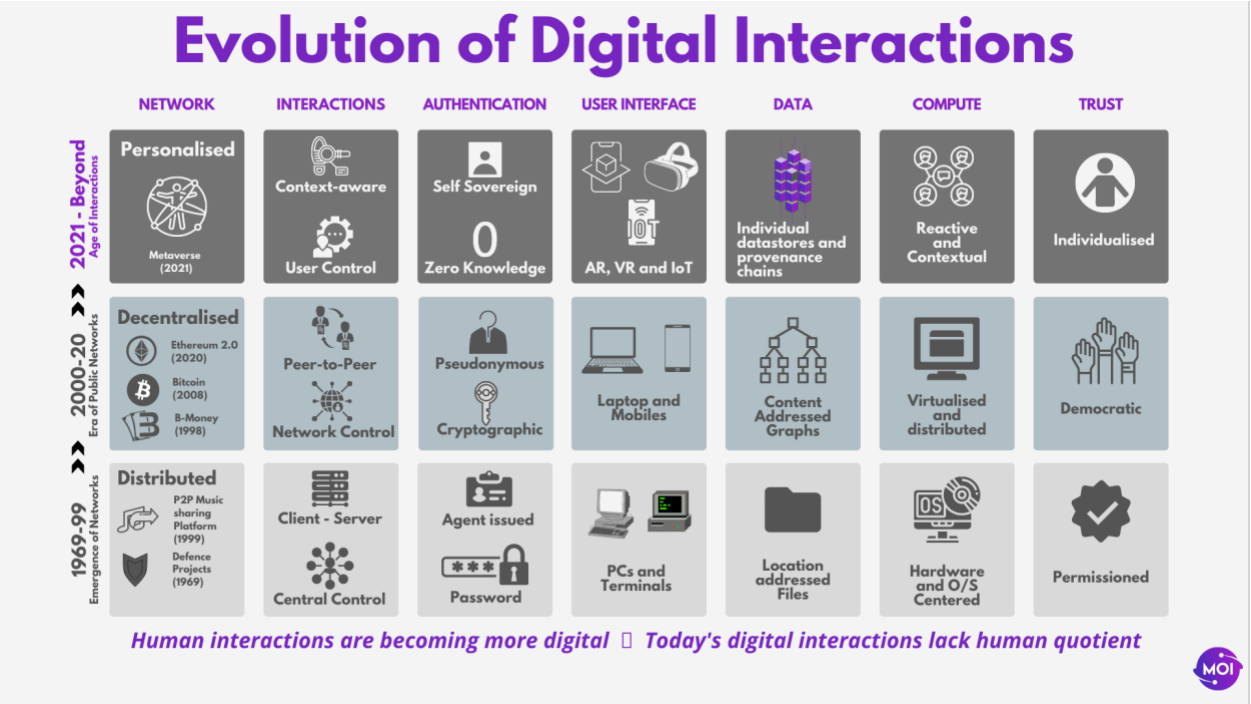
However, the decentralized protocols and blockchain networks of today are inadequate in meeting this requirement, as they rely on a systemic and programmatic approach for state management that is disconnected from participants and their preferences. This has led to a trade-off between security, scalability, and sustainability, resulting in multiple layers of blockchain networks and a complex and impractical solution. This lack of coherence makes it difficult to achieve a simple and unified internet of value. To enable sustainable, practical, equitable, and fulfilling interactions in the emerging digitally-connected society, Web3 needs to evolve fundamentally and enable human-like digital interactions.

State of today's web3 and rise of Intelligent Interactions

Today's blockchain systems are app-centric and built to manage thousands of cryptocurrencies using a static programmatic model**.** To meet the demand of billions of digital assets and dynamic user preferences in a peer-to-peer interaction model, we need a new solution. Unfortunately, this demand has resulted in islands of Web3 capabilities and a vast number of heterogeneous blockchain networks, each with its own app for each participant's unique need and situation. This is leading to a model with millions of bridges, roll-ups, and side-chains resulting in an insecure and impractical end-state.

In today's blockchains, even though participants own the values being managed, they are structured at the application level. For example, in the currently proposed web3 end-state, a person who uses digital for everyday living, like Uber for transport, Grubhub for food, Uniswap for finance, Facebook for social media, Twitter for messaging, and so on, will have their values created and managed in independent app-specific blockchains in the future. This situation will be even more challenging in a digitally interacting world with billions of assets and capabilities that will need to be supported in an inter-operable manner.

With the world operating using digital, every dimension of human value will require its own app and chain in the current Web3 model. However, these values belong to the same individual, and their true utility lies in a composite view of all values, with the ability to dynamically inter-operate between them in an interaction based on personalized user preferences. Unfortunately, this is currently infeasible in today's Web3 model, which was built to support cryptocurrencies based on a model for managing information. Instead, Web3 needs to shift towards managing values, which is fundamentally participant-centric.



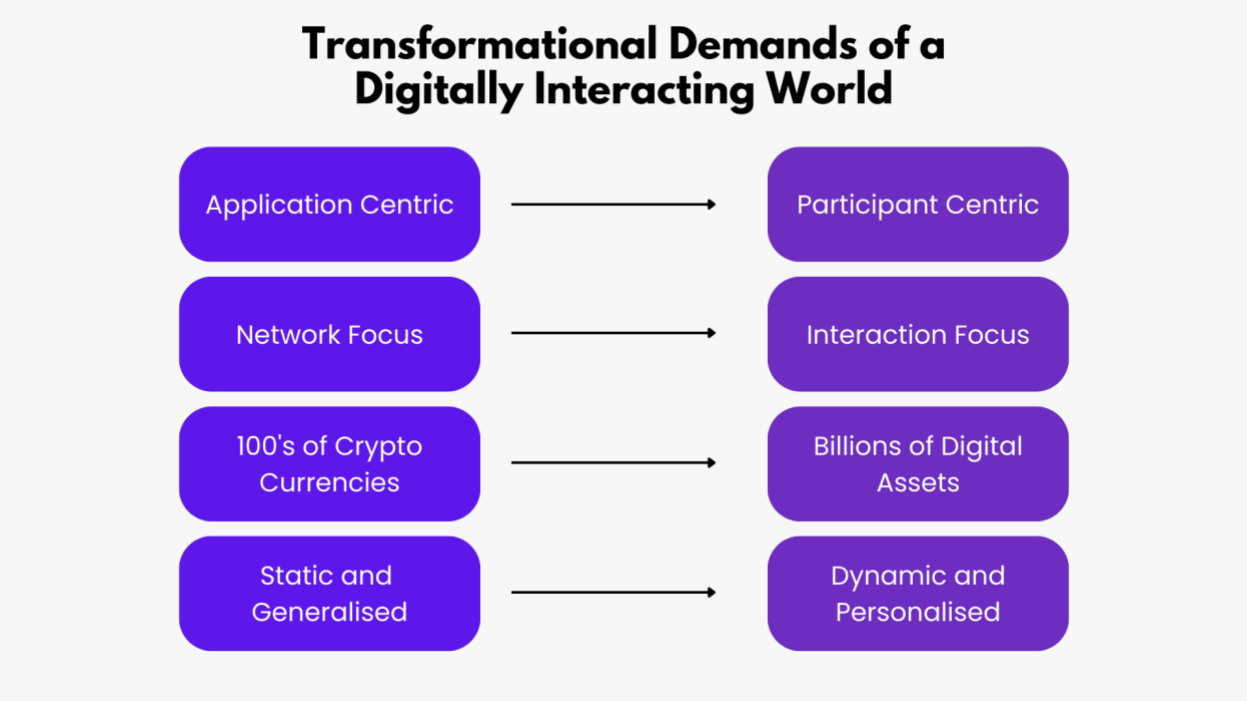
But the current blockchain networks, with their data structure, consensus model, and compute framework rooted in a programmatic and app-based approach, is struggling to keep up with the growth of an interactive p2p world. This is similar to what happened a decade ago with Bitcoin technology, which was unable to support multiple cryptocurrencies in the same network. As a result, smart-contract based networks like Ethereum emerged for multi-currency state management. It is now time for another evolution to meet the needs of the emerging digitally interacting society.

Technology transformation needed

As the digital world moves towards an interactive model, the demands on a general-purpose blockchain engine are becoming increasingly multi-dimensional, dynamic, and sophisticated. This requires a foundational rethinking of how state-management operates in the p2p world.

But todays' blockchain solutions, with their inability to pivot to an interaction model, are gearing towards a layered approach to this scalability problem, by moving the network load ,throughput demand , and compute sophistication to lower and lower chains . **This is creating enormous complexity for web3 adoption with significant compromise on security and sustainability of blockchain networks.**

The Digital Society is transforming



This is a foundational shift. What is needed is a true participant centric value creation and management in web3. What is needed is a fully participant-centric blockchain technology, from data structures to consensus to execution, all at a participant level to support the Integrated view of a user any time. In this model, interoperability becomes a foundational design not an afterthought. A network solution where support for dynamic user preferences, p2p interactions, and heterogenous asset management are design goals and not a system constraint. A network design in

which the side-chains, shards, and roll-ups are a choice, not a necessity. **A network model where the end-state is a flat internet like network with millions of nodes supporting billions of transactions; not a layered walled-garden approach of today.**

In summary, societal use of technology and its role has transformed, but the technology has not transformed to support this change. Technology is no longer just a tool; it is embedded in our everyday lives. What is needed is not a better engineering mouse trap, however sophisticated it may be. What is needed is a foundational rethinking of how computing and networks will work in the emerging digitally interacting world. A network that enables but doesn't control, where personalization is part of the network's fabric, not an app feature.

What is needed is a **simple participant-centric general-purpose blockchain technology .**

Our Solution

INTERACTION STATE MACHINE (ISM)
&
CONTEXT-AWARE BLOCKCHAIN NETWORKS

Solution Summary

Using our patented **'contextual compute'** model and ISM state machine replication technology specifically built for the digitally interacting world, MOI protocol enables a context-aware general-purpose blockchain network with millions of nodes and native inter-operability to support billions of interactions and digital assets with total personalization and complete user ownership and control.

MOI is a truly general purpose blockchain that can be personalized for all business contexts. It provides the flexibility and scalability of a cloud solution with the security of an L1 blockchain.

MOI delivers this capability by creating a **participant centric consensus** (PoXt), an **asset relevant data structure** (MDAG), and an **Interaction specific execution model** (PISA) to deliver a simple, scalable, secure, and sustainable end-state. Contrast this to today's app-centric and network-wide consensus, system focused data structure, and a programmatic (app sensitive) execution model.

Today's blockchains support multi-purpose capabilities centered around apps, what will be needed are general-purpose capabilities centered around participants. This is the transformation MOI is enabling.

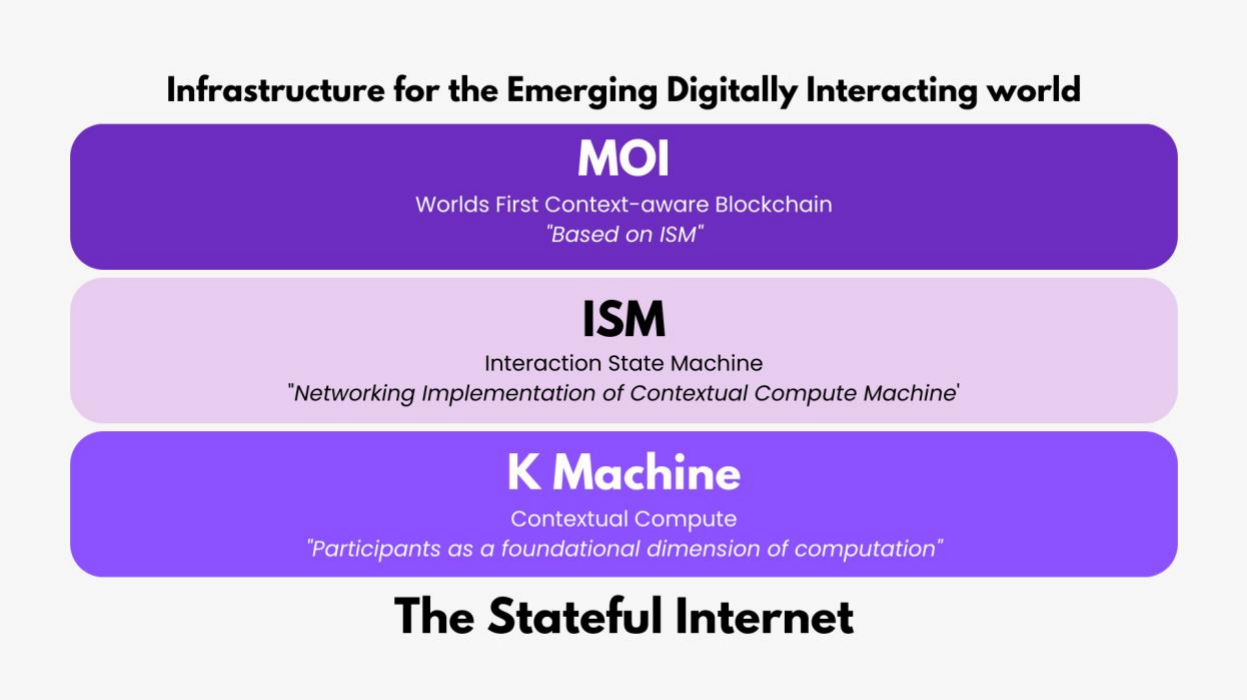
MOI is built for the Network world where value and states are network & participant attributes; today's block chains are built for a siloed world where values and states are node & app attributes.

Welcome to the world of "contextual compute".

Interaction State Machine

Interaction State Machine (ISM) is a new state machine replication technology that aims to support the needs of today's digitally interacting society. Through the revolutionary concept of contextual compute machines, ISM introduces participants into computing, enabling human-like digital interactions and a stateful Internet that is simple, secure, sustainable, and personalized.

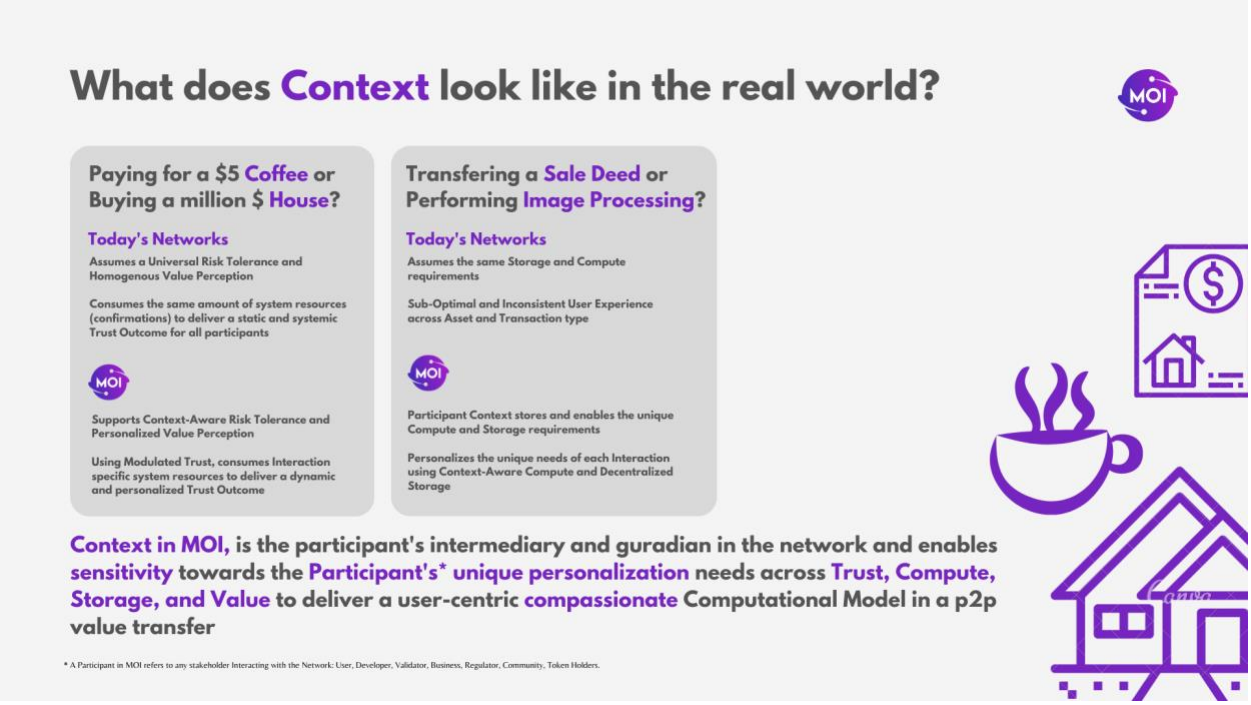
Unlike traditional state management of today's blockchain networks, ISM associates the state of an object with a participant and their state management preferences across the entire network. This facilitates true peer-to-peer and interaction-centric computing, delivering a simple, hyper-scalable decentralized network with growing security and seamless interoperability.



By using the idea of context, ISM creates a TCP-like framework for the stateful web, enabling a practical messaging paradigm for value creation, discovery, and management. Overall, ISM represents a significant shift in how computing is done, emphasizing the importance of participants and context in delivering a more user-friendly, efficient, and secure digital experience.

Context

The fundamental principle of ISM is based on the concept of "Context." Context is a groundbreaking computing element that puts the participant at the center of computation in ISM. Essentially, Context serves as the participant's representative in the network. It adapts and expands as the participant engages with the network and with other participants.



Context Object

ContextObject is an autonomous object that establishes the relationship between a content and its context in the network. It is comprised of two components: Content, which represents the value that must be managed in the network, and Context, which refers to the most recent context associated with the content. ContextObject serves as the core state management component in ISM.

Context Super State

ISM utilizes Context Super State to handle value transfers in blockchain networks. It is a composite state vector that serves as a cryptographic primitive to represent the participant's most recent state in ISM. Context Super State comprises all the context objects that the participant manages and the systemic context objects that the participant possesses or owns.

KRAMA

Krama is a participant-centric ordering and agreement mechanism that is built based on context. It serves as the foundational data agreement mechanism of ISM and is based on personal context clocks, eliminating the need for a network-wide system clock in a distributed system. This enables hyper-concurrency and infinite scalability in ISM based chains.

MOI – Practical Implementation of ISM

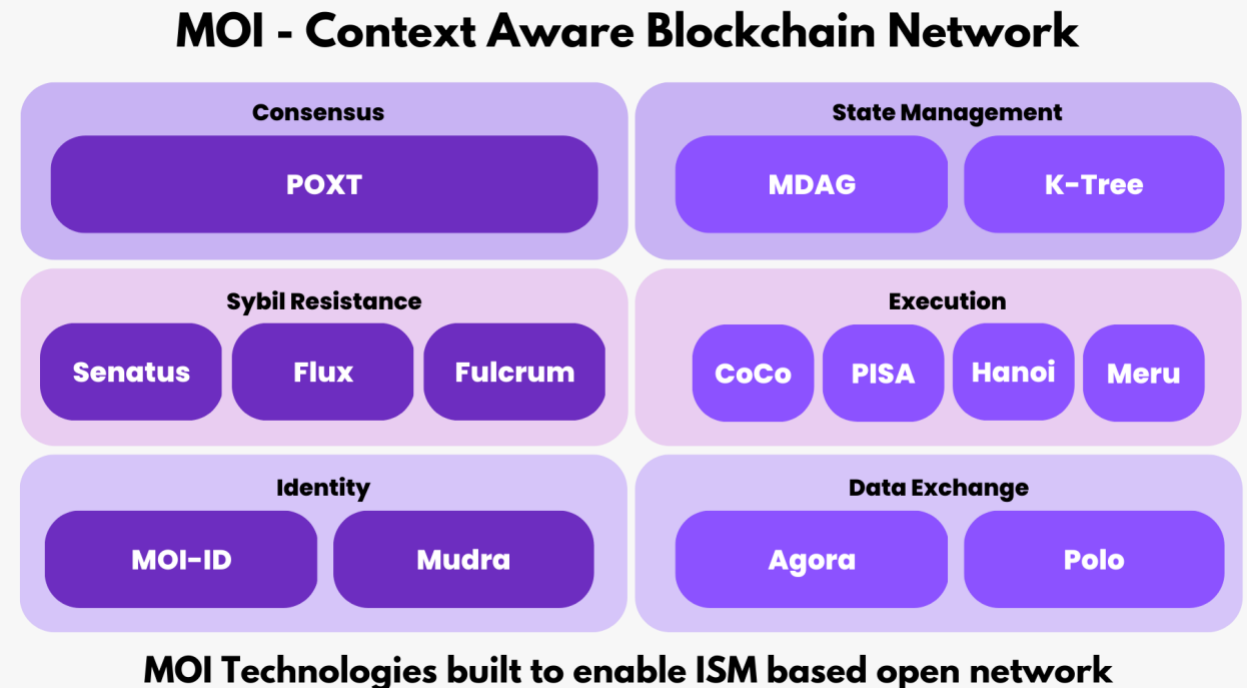
World's first Context-aware P2P protocol and network

MOI is the world's first context-aware p2p protocol and open blockchain network based on ISM. Using the fundamentally new idea of 'contextual computation', MOI brings participants as a foundational dimension of computation to humanize the internet and propel the emerging digitally interacting society to be equitable, democratic, simple, and sustainable.

A p2p protocol and an open network that is participant centric, MOI allows users to dynamically control their identity, compute, storage, trust, and digital assets based on their unique needs. It employs a novel consensus algorithm aiming to facilitate billions of interactions in a secure and sustainable fashion across millions of nodes.

MOI is the first decentralized network that functions as a truly global value network. It places the utmost trust in the participants themselves, using their unique context as the key resource for locking and synchronization. This makes MOI network highly parallelized, ensuring speed and efficiency without sacrificing security or decentralization.

Components of MOI



State Management: MDAG

MOI implements state management using a path-breaking participant centric multi-dimensional data structure called **MDAG.**

MDAG (Multi-level Composite DAG) enables creation and management of Context Objects in MOI. It is a participant-centric intelligent data structure to independently manage the compute, storage, and multi-dimensional values of an interaction.

MDAG supports:

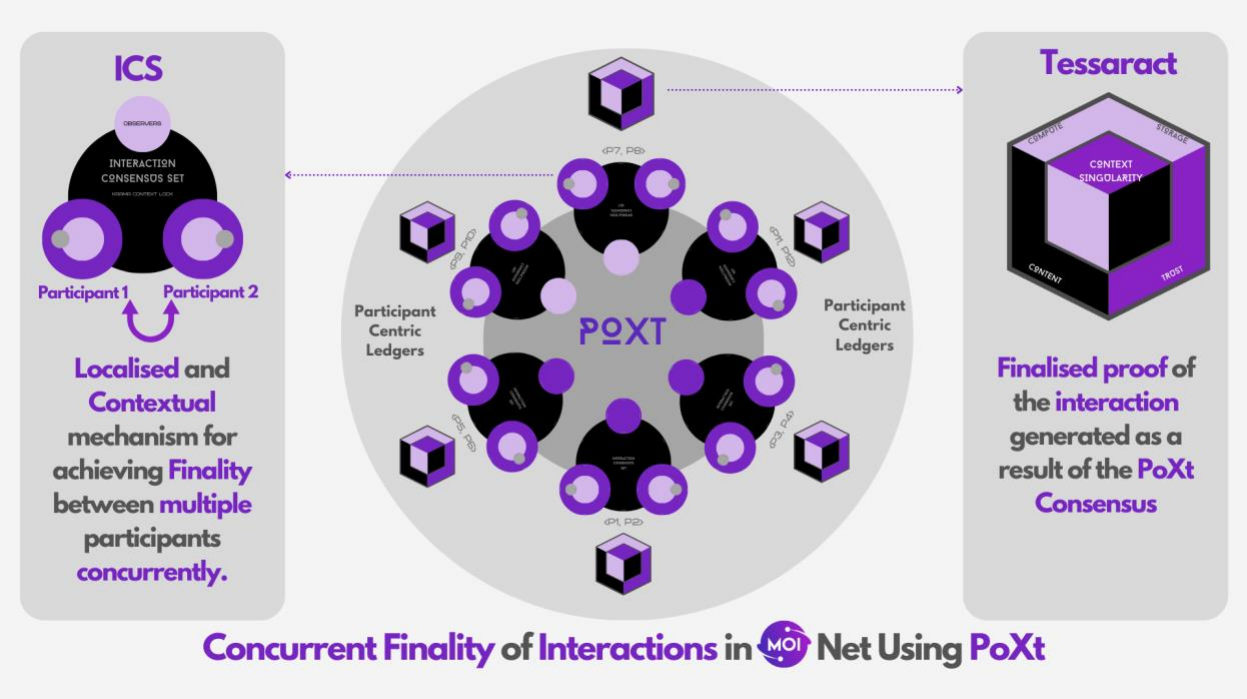
- Participant-level state management by **"Transition links"**
- Network-level state management by **"Interaction links"**

allowing simultaneous creation of total ordering at a participant and network level. The MDAG data structure delivers light speed finality using the transition links and network level security using the Interaction links. With this transformational ability to focus both on objects and network simultaneously and independently, MDAG brings the best of both account and UTXO models to public blockchains for the first time and delivers unparalleled scalability and hyper concurrency while maintaining maximum security. Using this revolutionary MDAG structure, MOI solves the fundamental data structure limitations of today's blockchains.

Consensus: Proof-Of-Context (PoXt)

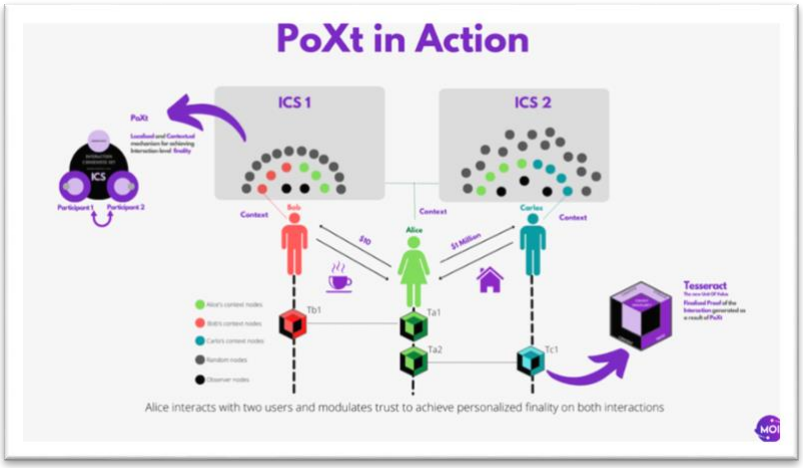
Krama based P2P Consensus engine for open systems with support for Byzantine fault tolerance. PoXt is based on Krama, the participant centric ordering mechanism, enables hyper concurrency, long term decentralization, and simple sustainability with no central bottlenecks.

PoXt leverages the Context of Interaction participants to achieve global finality of participant's network states in a single-step. By utilizing nodes, themselves as an intermediary resource, PoXt achieves light-speed global finality and hyper consensus, delivering true linear scalability and efficient network utilization. To support hyper scalability PoXt virtualizes the Byzantine agreement process using context and delivers dynamic personalization to participants by modulating the trust requirements based on interaction specifications.



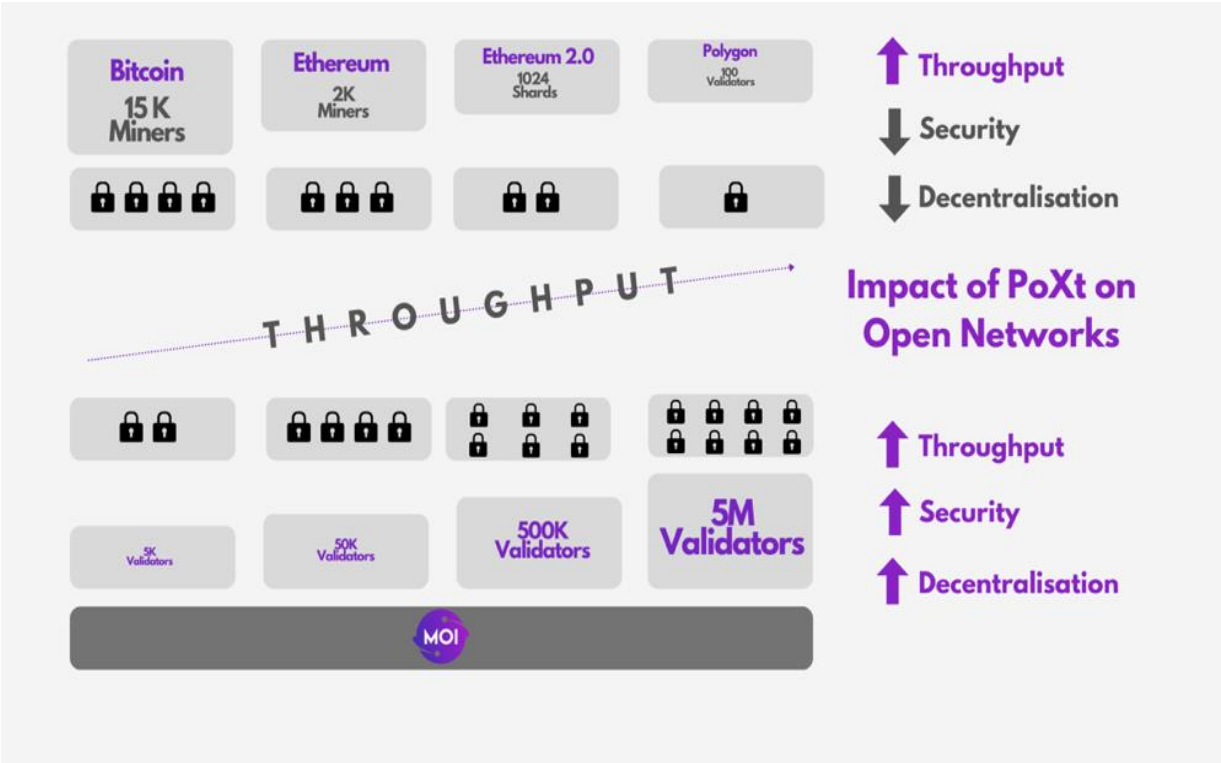
To achieve scalability and efficiency, PoXt utilizes an advanced stochastic model that harnesses the dynamically changing network entropy. This delivers the scalability benefits of a leaderless consensus model while retaining the speed and sustainability advantages of a leader-based consensus model.

Pictorial representation of a value transfer in MOI using PoXt



PoXt has significant implications for the development of scalable, decentralized networks. Its participant-centric approach, efficient utilization of network resources, and innovative sybil-resource model ensure equitable participation and long-term sustainability, while its linear scalability and hyper-consensus mechanism provide a foundation for the next generation of high-performance decentralized applications.

MOI provides scalability and throughput without sacrificing security and decentralization.



Execution: PISA

A personalized Virtual Machine (PVM) to simply and safely support the dynamic execution needs of Interaction Centric Compute. PISA is an Interaction specific virtual machine enabling context-optimized computation.

PVM enables true general-purpose blockchain execution by balancing flexibility and risk to deliver customizable user-ownership and control based on Participant context and Interaction preferences. PISA supports 4 orders of state management with increasing degrees of general-purpose(ness):

Order 1: Code-less . No code State Management
Order 2: Network Coded . Protocol enabled State Management
Order 3 : User Coded . Logic enabled State Management
Order 4 : Dynamically coded. Personalized state Management

In MOI, most of today's asset and token management smart-contracts can be implemented as Order 1 Interactions without writing any code, significantly increasing the security, and decreasing the complexity for developers.

COCO – Context Oriented Compute Language

Cocolang is a secure, deliberate, and developer friendly programming language for MOI. It is a statically typed, high-level context-oriented programming language for developing Logics in MOI and can compile multiple runtime engine targets. The primary design philosophy for COCO is safety, security, and ease of use which it achieves using a highly readable syntax with highly intentional logic expressions i.e., it is very difficult to write something with ambiguous meaning in Coco.

Sybil Resistance

Senatus

A participant specific resource enabling context aware Sybil resistance for democratic network participation

Flux

Flux is a randomization algorithm which harnesses the natural entropy of the network. It is based on an intelligent and novel multi-step stochastic mechanism for true random sampling.

Fulcrum

Fulcrum is a Context-enabled load balancer for equitable and sustainable network participation. Fulcrum makes sure that honest validators in the network get enough work and are able to equitably share the value generated.

Data Exchange

Agora

A context addressed data access mechanism allowing for Interaction level finality and global data availability. Agora also provides an integrated file management capability.

POLO – Prefix Ordered Lookup Offset

A wire efficient light weight serialization format supporting partial and differential messaging to optimize the network load generated by hyper concurrency.

Identity

MOI-ID

A decentralized identity which acts as the 'Digital Persona' of the participant with built in inter-operability. MOI-ID is the foundational identity element in MOI and all other elements are linked to this.

MUDRA

Context relevant signature schemes and a zero-knowledge based solution to manage participant's interactions in MOI and across other chains.

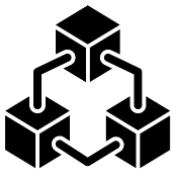
Benefits of MOI

MOI is a general-purpose blockchain protocol centered around participants and specifically built for the emerging digitally interacting world. MOI is an infinitely scalable and secure Layer-1 network, enabling anyone to easily deploy assets and applications catered to specific and dynamic user needs.

Value proposition to different stakeholders

Developers with a **user-friendly, secure**, and **low-code** environment for easy adoption of web3 technology. MOI provides the flexibility of a cloud with the security of a decentralized blockchain.

Enterprises can benefit from **a practical** and **sustainable** web3 solution that is fully **customizable** to their specific needs, providing complete ownership and control. This allows them to easily manage both privacy and transparency on a single network, based on the context of their interactions and applications.



Technologists with the ability to create **scalable** solutions **without compromising on security or decentralization.**

Key functional benefits

1. **Infinitely scalable, Secure, and personal**
   With MOI you can have flat network of millions of nodes supporting billions of assets and interactions. Shard-chains, Sidechains, and rollups are optional and not a necessity for scaling making the network simple, secure, and sustainable. The context-aware model of consensus and execution, makes MOI faster than a database, more flexible than Ethereum and as safe as Bitcoin.

2. **General purpose**
   With an Interaction centric execution model and Participant centric state management MOI decouples state and code to support all applications, from DeFi, gaming, storage, to Web3 computing in a single chain with dynamic participant preferences

3. **P2P & Interactive**
   Transfer all tokens natively at a p2p level. App, asset, and personal tokens get the same first order security of the protocol tokens like ETH & BTC. The proof-of-context consensus eliminates the need for a systemic global state and supports hyper-concurrency and p2p value transfers for all tokens.

4. **Simple for Users**
   We re-invented blockchain to save you from side chains, shard chains and the need for 'zillions of app chains.' No more complex and unsafe bridges; everything revolves around the participant. All your assets stay with you, and come with you, not in someone else's smart contract. Makes it safe, simple, and personal

5. **Context Aware & Interoperable**
   Transact across millions of nodes with billions of transactions based on your own digital footprint in a single flat-chain. Context, the new participant level super-state, will allow for a user to work across networks easily and seamlessly with the ability to safely transfer assets and values from one person to another person in any chain.

Differentiated Used Cases

1. **Safe Defi**
   MOI enables user-controlled peer-to-peer value transfer of any token or currency. In traditional blockchain networks, a participant's values are stored in a token smart contract, which poses a significant security risk due to the potential for a "honey pot" attack. In contrast, MOI **decouples the code and value**, storing the token values at a participant level. This approach ensures that the framework for delivering decentralized finance (DeFi) solutions is extremely secure.

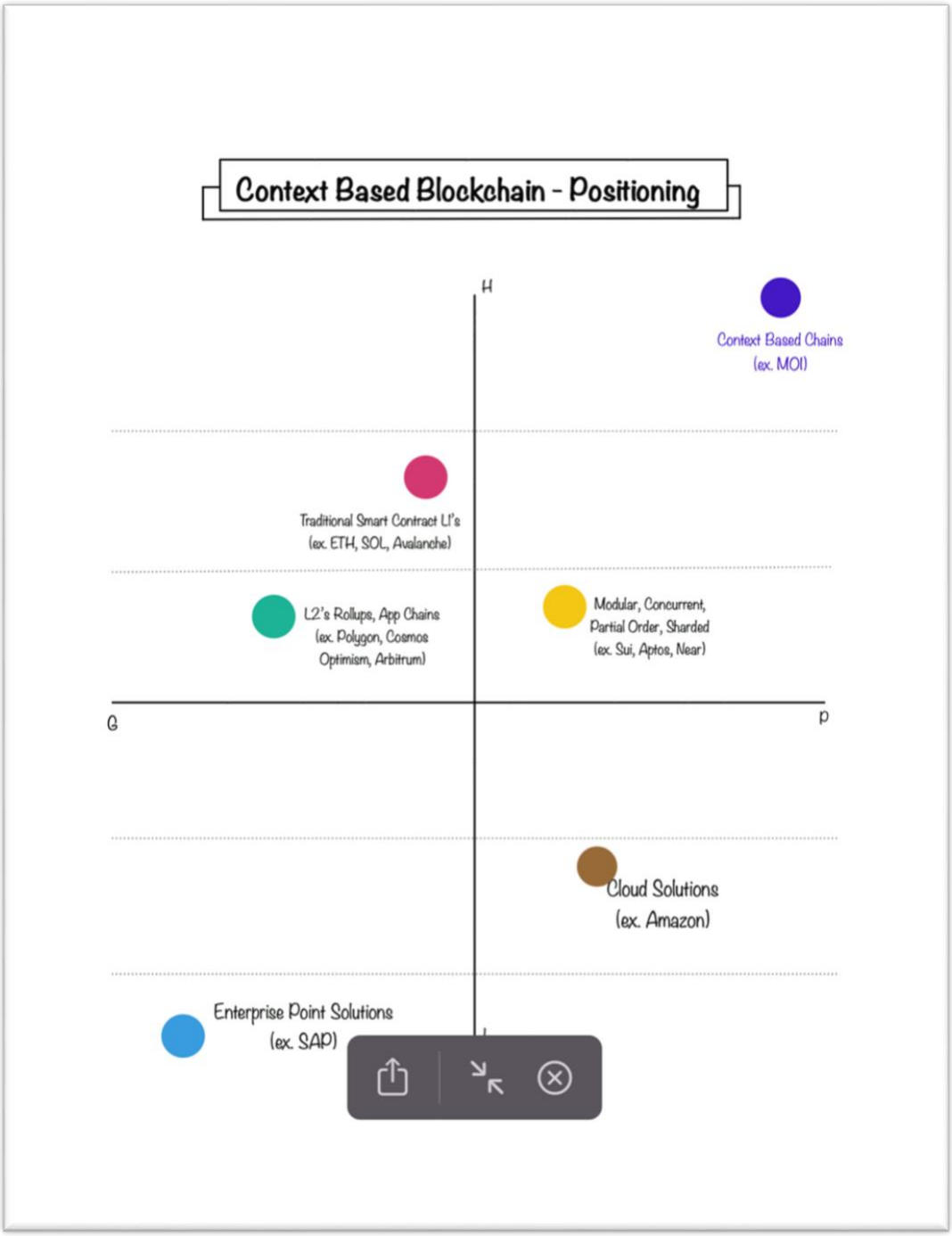
2. **P2P Interactions with Native Interoperability e.g., P2P gaming**
   MOI allows for all interactions and digital assets to be owned and **interoperated** at the **participant level**, making it possible for gamers to move their assets seamlessly across multiple chains without requiring complex bridges and connectors. This results in a simplified user experience and enables game creators to develop more **dynamic**, participant-focused business models instead of focusing solely on assets. This native interoperability also allows for more simplified user experience for gamers, making it easier to move their assets across different chains.

3. **Practical Provenance**
   In today's blockchain networks, provenance capabilities are typically integrated with smart contracts. This limits their applicability in existing ecosystems such as supply chains since all parties involved need to be blockchain-enabled. Moreover, this tightly coupled nature only allows for tracking the provenance of states managed in the ledger and not for other objects like files, making blockchain adoption in enterprises impractical. MOI addresses this challenge by **decoupling** the **identification, storage, and ledger** components and tying them together at a participant level. This enables the **provenance of both state and data management**, delivering a practical solution for enterprises and businesses.

POSITIONING

Evolution of Blockchain Networks

	Transactional	Programmatic	Interactive
Asset	Single currency	Multi-currency	**Millions of assets, heterogenous values**
Focus	Asset Centric & transfer	App Centric & programmatic	**Participant centric & context-aware**
Use	Single-purpose	Multi-purpose	**General Purpose & Personalized**
State Model	Single Global State	Single Global State	**Participant Global State**
State Vector	UTXO	Smart-contract	**Context Super State**
Tokens	Single	Multiple & programmatic, not protocol native	**Multi-dimensional and personal, Protocol Native**
Consensus	POW	POS, POW	**POXT**
Data Structure	Blockchain	Blockchain, Graph	**MDAG, Tesseract**
Compute	Script	Programmatic	**Interactive**
VM type / focus	None	Programmatic / Turing Complete	**General purpose/ Simplicity, Safety**
Network size	1000's of nodes	1000's of nodes	**Millions of nodes**
Network Growth	Flat	Layered	**Flat**
Interoperability	N/A	Bridges	**Direct**
Performance (TPS)	100's	1000's	**Millions**
Network Usage	Simple	Complex	**Simple**
Sustainability - Energy	Red	Green	**Green**
Sustainability -Scalability	Difficult	Possible with Complexity and reduced security	**Infinite and secure**
Sustainability -Equity	Long term Centralization	Long term Centralization	**Long term Decentralization**
Network (validator) participation	Complex	Complex	**Simple**
Chains	BTC ++	ETH ++	**MOI ++**



x-axis	Degree of Scalability & Flexibility	#assets, # of apps, TPS, Interaction Maturity, degree of Dynamicity,P2P support
y-axis	Degree of security & Decentralization	# of nodes, # of operators, Hardware Complexity, Environmental Impact, Ease of Sybil resource /network participation

Social Impact

The MOI blockchain network is both sustainable and democratic. It achieves this through its participant-centric sybil resistance resource and PoXt consensus algorithm, which enable global participation in the network using simple hardware. This significantly reduces the carbon footprint of the network, making it more environmentally friendly. Additionally, this approach promotes equity in the digitally interacting society by allowing more people to participate in the network regardless of their technical expertise or financial resources.