The official wallet of Supra.

DOWNLOADNOW




- Products

**Research Focus**

## We're solving blockchain trilemmas

All blockchain solutions are designed with cryptographic and distributed computing primitives, but their designs vary in terms of speed, security, and decentralization. Most have had to face the trilemma of choosing a trade-off between these qualities. Our research team's core focus has been to devise protocols that resolve this trilemma once and for all. We're building solutions that harness better performance at lower costs with higher degrees of decentralization and security. That's the principal problem we're cracking at the cryptographic, protocol, and crypto-economic design level.

PLAY OVERVIEW VIDEO

SUPRATECH | Research Areas | Media | Publication library

## The tech behind Supra

Explore our solutions and how they apply with our growing series of Whitepapers.

Supra 2.0

The AutoFi Vision

**Supra 2.0**

DOWNLOAD WHITEPAPER

Supra Research unveils its most ambitious vision yet: Automatic DeFi. This paper shows how Supra's vertically integrated Layer-1—complete with native oracle feeds, deterministic on-chain automation, and seamless cross-chain messaging—turns every block into a self-governing financial engine. Discover core AutoFi primitives, our transparent auction revenue model, and the path to a living, reflexive capital system.

FIRST PUBLISHED: MAY, 2025

|

Share Whitepaper COPY LINKhttps://supra.com/documents/Supra-AutoFi-Whitepaper.pdf

Developers

racles

Oracle Protocol

Archived copy · cryp2nova.com

## Threshold AI Oracles

The official wallet of Supra.

DOWNLOAD WHITEPAPER

In this whitepaper, we show how just-in-time query triggers fire only when on-chain conditions demand, how decentralized committees of specialized AI agents deliberate in parallel to deliver bias-resistant insights, and how BLS threshold signatures bundle their verdicts into compact, verifiable proofs—unlocking fully autonomous, secure DeFi automation without any off-chain keepers.

FIRST PUBLISHED: MAY, 2025

|

Share Whitepaper COPY LINKhttps://supra.com/documents/Threshold_AI_Oracles_Supra.pdf

Supra Overview Whitepaper

SUPRATECH

### Supra Overview Whitepaper

DOWNLOAD WHITEPAPER

Supra Research has put out 10+ papers for a wide range of blockchain protocols so far, this overview master whitepaper showcases how it all comes together and works on Supra Layer 1. It takes you through our native oracle services, MultiVM capabilities, Supra Containers, novel Tribes and Clans network design, Moonshot Consensus, transaction flow, parallel execution strategies, and much more. Read the full paper for an end-to-end overview of Supra Layer 1.

Ecosystem

FIRST PUBLISHED: November, 2024

|

Share Whitepaper COPY LINKhttps://supra.com/documents/SupraTech-Whitepaper.pdf

Moonshot Consensus Algorithm

PLAY VIDEO

Learn

Consensus Protocol

### Moonshot Consensus Algorithm

Read Litepaper Download Whitepaper

Introducing Moonshot, a new family of high throughput, low latency blockchain-based SMR protocols characterized by Optimistic Proposal. We primarily cover Chained Moonshot, a variant of Moonshot that relies on vote broadcasting and QC Chaining.

Archived copy · cryp2nova.com

In our experiments, Chained Moonshot produced 54.9% higher throughput and 41.1% lower latency than Diem, a state-of-the-art blockchain-based SMR protocol.

First Published: July 12, 2023

View Presentation Deck

Share Whitepaper COPY LINKhttps://supra.com/documents/Moonshot-Whitepaper.pdf

Supra IntraLayer

Community

### Supra IntraLayer

DOWNLOAD WHITEPAPER

Supra IntraLayer is a comprehensive two-layer infrastructure for developers to create decentralized autonomous agents, comprised of a multipurpose decentralized network with native services as well as enshrined DeFi protocols. It facilitates trustless automation and provides comprehensive, seamless solutions for asset management and financial services throughout the digital finance landscape.

FIRST PUBLISHED: June, 2024

About

Share Whitepaper COPY LINKhttps://supra.com/documents/Supra-IntraLayer-Whitepaper.pdf

Supra Containers

PLAY VIDEO

Appchain Model

### Supra Containers

n More Download Whitepaper

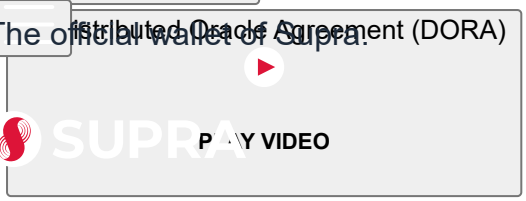
Presenting Supra Containers, a unique appchain model that creates flexible pockets of dedicated blockspace within Supra L1, reserved for current and future throughput needs of dApps. Containers gives builders a great deal of freedom and control to customize their gas fees, gas tokens, and governance. It lets them create appchain-like experiences at a fraction of the cost, with a much simpler setup process.

FIRST PUBLISHED: September, 2024

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com

UILD ON SUPRA
COPY LINKhttps://supra.com/documents/Supra-Containers-Whitepaper.pdf
The official wallet of Supra!




Oracle Protocol

**Distributed Oracle Agreement (DORA)**

Read Litepaper | Download Whitepaper

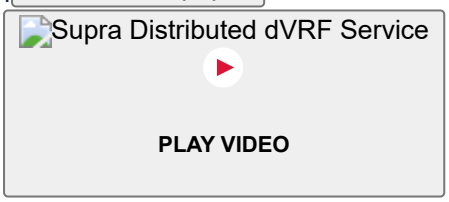
Presenting our novel Distributed Oracle Agreement (DORA) protocol - a highly resilient and efficient oracle protocol.
In this paper, we describe how agreement distance allows us to redefine agreement among nodes and how leveraging State Machine Replication (SMR) allows us to tolerate Byzantine failures of up to 49% in our DORA protocol.

First Published: JANUARY 26, 2023

|

View Presentation Deck

| Share Whitepaper COPY LINKhttps://supra.com/documents/DORA-Whitepaper.pdf




dVRF Protocol

**Supra Distributed dVRF Service**

Read Litepaper | Download Whitepaper

Presenting Supra dVRF Service for generating verifiable random values in the Web3 ecosystem. We provide a smart-contract based flexible dVRF service framework, that is fully decentralized via a threshold cryptographic architecture.
It offers several new features - among them output-privacy, which enhances the utility of dVRF in the blockchain space and reduces the gas cost significantly.
First Published: January 26, 2023

|

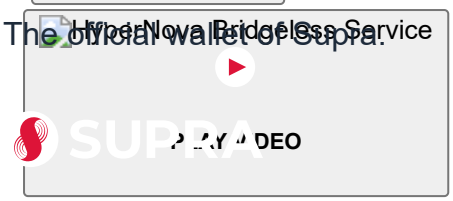
View Presentation Deck

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com

Share Whitepaper COPY LINKhttps://supra.com/documents/VRF-Service-Whitepaper.pdf

The official wallet of Supra.




- Cross-chain Bridgeless Consensus

**HyperNova Bridgeless Service**

Read Litepaper Download Whitepaper

- HyperNova is a trustless bridge design wherein the bridge nodes only act as relayers and NOT as validators of information so that the source and destination chain themselves validate the events from the other chain. This removal of the possibility of the corruption by the (middlemen) bridge nodes yields a higher level of security than of multi-sig bridges, of the level of source and destination chains.

FIRST PUBLISHED: October 27, 2023

|

Share Whitepaper COPY LINKhttps://supra.com/documents/Supra-HyperNova-Whitepaper.pdf

## The $SUPRA Token

- 
- 
- Supra will be a cross-chain IntraLayer, enabling automation across Web2 and Web3 via secure and scalable smart contract interoperability — with the $SUPRA token harmonising incentives of all network participants.
- In this document, we highlight Supra’s overarching vision and the expanded utility of the $SUPRA token.

Download PDF Document

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com



The official wallet of Supra.



## Our research areas

We're working on multiple, interconnected areas.

Distributed protocols

- Consensus Protocol
- Reliable Transaction Dissemination
- Distributed Oracles
- Sharding

Cryptography

- On-chain Randomness
- Zero Knowledge
- Multi Party Computation
- Verifiable Computing
- Key Management & Recovery

DeFi / TradFi

- Tokenomics
- Crosschain DEX
- Market Makers
- Proof of Liquidity
- Bridges

Security

- Software Testing
- DevSecOps
- Internal Audits

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com

- Crypto-economic Security

The official wallet of Supra.

Parallel Execution

- Multi core execution
- Containers
- Access-Specification based execution

Programming Languages and Formal Methods

- Compilers
- Program Analysis
- Formal Verification of Distributed Protocols
- Theorem Proving
- Model Checking

## Watch our research walkthroughs

PLAY VIDEO

SUPRA TECH

Supra Abstraction

CRYP2NOVA

**Dr. Aniket Kate**

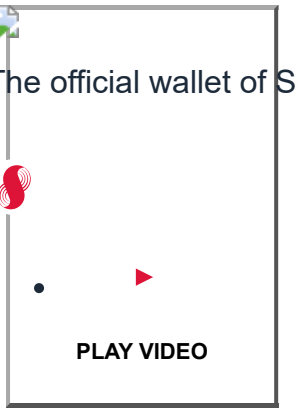
An introduction to Supra's research breakthroughs in blockchain protocol designs with a quick overview by Dr. Aniket Kate, our Chief Research Officer and research team lead.

Video length: 9mins

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com

The official wallet of Supra.




Oracles

- Distributed Oracle Agreements (DORA)

**Dr. Saurabh Joshi**

In this video, Dr. Saurabh Joshi describes how agreement distance allows us to redefine agreement among nodes and how leveraging State Machine Replication (SMR) allows us to tolerate Byzantine failures of up to 49% in our DORA protocol.

- Video length: 24mins




dVRF Protocols

- Supra Distributed dVRF

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

**Dr. Pratyay Mukherjee**

- Dr. Pratyay walks us through a smart-contract based flexible dVRF service framework, that is fully decentralized via a threshold cryptographic architecture.

Archived copy · cryp2nova.com

It offers several new features - among them output-privacy, which enhances the utility of dVRF in the blockchain setting, and reduces the gas cost significantly.

Video length: 18mins

PLAY VIDEO

Consensus Protocol

Moonshot Consensus

**Dr. Raghavendra Ramesh**

**Isaac Doidge**

In this video, we introduce the Moonshot Consensus protocol, a new family of high throughput, low latency blockchain-based SMR protocols characterized by Optimistic Proposal.

Video length: 20mins

## Publication library

Read selected works by Supra's world class researchers to learn more about what makes our team tick.

SUPRATECH

All Papers

Publications

Preprints

SUPRATECH |Publication

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com

**Hydrangea++: Enhancing Hydrangea with Optimistic Proposals**

The official wallet of Supra.

Nibesh Shrestha and Aniket Kate

FIRST PUBLISHED: November 2025 | Share https://supra.com/documents/hydrangea-plus-plus.pdf

SUPRATECH |Publication

**Blockchain Transaction Conflicts: A Historical Perspective**

Parwat Singh Anjana, Srivatsan Ravi

FIRST PUBLISHED: FEBRUARY 24, 2025 | Share https://arxiv.org/pdf/2505.05358

SUPRATECH |Publication

**Efficient Parallel Execution of Blockchain Transactions Leveraging Conflict Specifications**

Parwat Singh Anjana, Srivatsan Ravi, Raghavendra Ramesh, Joshua Tobkin, Rohit Kapoor, Matin Amini, and Rahul Parmar

ACM Advances in Financial Technologies (AFT'25)

FIRST PUBLISHED: FEBRUARY 24, 2025 | Share https://drops.dagstuhl.de/storage/00lipics/lipics-vol354-aft2025/LIPIcs.AFT.2025.29/LIPIcs.AFT.2025.29.pdf

SUPRATECH |Publication

**Block Transactional Memory: A Complexity Study**

Parwat Singh Anjana, Srivatsan Ravi

The 27th International Symposium on Stabilization, Safety, and Security of Distributed Systems

FIRST PUBLISHED: FEBRUARY 24, 2025 | Share https://supra.com/documents/Supra-Block_Parallelization_Lower_Bound-Whitepaper.pdf

SUPRATECH |Publication

**Towards Improving Throughput and Scalability of DAG-based BFT SMR**

Nibesh Shrestha and Aniket Kate

European Conference on Computer Systems (EuroSys) 2026

LATEST VERSION: May 19, 2025 | Share https://eprint.iacr.org/2025/877.pdf

SUPRATECH |Preprint

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com

**Hydrangea:Optimistic Two-Round Partial Synchrony**

The official wallet of Supra.

Nibesh Shrestha, Aniket Kate, and Kartik Nayak

LATEST VERSION: JULY 10, 2025 | Share https://eprint.iacr.org/archive/2025/1112/1752115676.pdf

SUPRATECH |Preprint

**Fused Token Offering (FTO)**

Arman Abgaryan, Utkarsh Sharma and Joshua Tobkin

FIRST PUBLISHED: JUNE 2025 | Share https://supra.com/documents/fused-token-offering.pdf

SUPRATECH |Preprint

**Optimistic, Signature-Free Reliable Broadcast and Its Applications**

Nibesh Shrestha, Qianyu Yu , Aniket Kate, Giuliano Losa , Kartik Nayak and Xuechao Wang

32nd ACM Conference on Computer and Communications Security (CCS), 2025

LATEST VERSION: May 2025 | Share https://arxiv.org/pdf/2505.02761

SUPRATECH |Preprint

**InstaRand: Instantly Available and Instantly Verifiable On-chain Randomness**

Jacob Gorman, Lucjan Hanzlik, Aniket Kate, Pratyay Mukherjee, Pratik Sarkar and Sri Aravinda Krishnan Thyagarajan

LATEST VERSION: May 19, 2025 | Share https://eprint.iacr.org/2025/896.pdf

SUPRATECH |Publication

**Which Signature Scheme to Pick for Your Distributed Protocol?**

Aniket Kate, Pratyay Mukherjee, Hamza Saleem, Nibesh Shrestha

LATEST VERSION: April 2025 | Share https://supra.com/documents/SupraTech-Signature-Benchmarking.pdf

SUPRATECH |Preprint

**Dyna-hinTS: Silent Threshold Signatures for Dynamic Committees**

Aniket Kate, Pratyay Mukherjee, Samipa Samanta, Pratik Sarkar

7th Crypto Valley Conference, 2025

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com

FIRST PUBLISHED: APRIL 07, 2025 | Share https://eprint.iacr.org/2025/631.pdf

The official wallet of Supra.

SUPRATECH |Preprint

**Access Specification Aware Software Transactional Memory Techniques for Efficient Execution of Blockchain Transactions**

- Parwat Singh Anjana, Srivatsan Ravi, Raghavendra Ramesh, Joshua Tobkin, Rohit Kapoor, and Rahul Parmar

FIRST PUBLISHED: FEBRUARY 24, 2025 | Share https://arxiv.org/pdf/2503.03203

SUPRATECH |Preprint

**Auto-Balancer: Harnessing idle network resources for enhanced market stability**

- Arman Abgaryan, Utkarsh Sharma

FIRST PUBLISHED: January, 2025 | Share https://arxiv.org/pdf/2502.20670

SUPRATECH |Preprint

**KeyClub and RandRec: Two New Social Key Recovery Schemes**

- Aniket Kate, Pratyay Mukherjee, Pratik Sarkar, Bhaskar Roberts, Hamza Saleem

FIRST PUBLISHED: Sept 27, 2024 | Share https://supra.com/documents/Supra-Key-Recovery.pdf

SUPRATECH |Preprint

**Supra Containers as App-Chains for Efficient Parallel Execution of Transactions**

- Raghavendra Ramesh, Joshua Tobkin, Parwat Singh Anjana and Saurabh Joshi

FIRST PUBLISHED: JULY 10, 2024 | Share https://supra.com/documents/Supra-Containers-Whitepaper.pdf

SUPRATECH |Preprint

**vRaaS: Verifiable Randomness as a Service on Blockchains.**

- {{JACOB_GORMAN}},Lucjan Hanzlik, Aniket Kate, Easwar Vivek Mangipudi, Pratyay Mukherjee, Pratik Sarkar and Sri Aravinda Krishnan Thyagarajan

38th IEEE Computer Security Foundations Symposium, 2025

FIRST PUBLISHED: JUNE 14, 2024 | Share https://eprint.iacr.org/2024/957

SUPRATECH |Preprint

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com

**ntraLayer: A Platform of Digital Finance Platforms**

The official wallet of Supra.

Arman Abgaryan, Utkarsh Sharma

FIRST PUBLISHED: June, 2024 | Share https://arxiv.org/pdf/2412.07348

SUPRATECH |Preprint

**Sailfish: Towards Improving the Latency of DAG-based BFT**

Nibesh Shrestha, Aniket Kate, Rohan Shrothrium and Kartik Nayak

46th IEEE Symposium on Security and Privacy, 2025

FIRST PUBLISHED: MAY 2, 2024 | Share https://eprint.iacr.org/2024/472.pdf

SUPRATECH |Publication

**Formally Verifying the Safety of Pipelined Moonshot Consensus Protocol**

Raghavendra Ramesh, Praveen Manjunatha and Isaac Doidge

FIRST PUBLISHED: March 25, 2024 | Share
https://drops.dagstuhl.de/entities/document/10.4230/OASIcs.FMBC.2024.3

SUPRATECH |Preprint

**HyperLoop: Rationally Secure Cross-chain Bridge**

Easwar V. Mangipudi, Joshua Tobkin and Raghavendra Ramesh

FIRST PUBLISHED: December 8, 2023 | Share https://supra.com/documents/Supra-Hyperloop-Whitepaper.pdf

SUPRATECH |Preprint

**Proof of Efficient Liquidity: A Staking Mechanism for Capital Efficient Liquidity**

Arman Abgaryan, Utkarsh Sharma and Joshua Tobkin

FIRST PUBLISHED: October 28, 2023 | Share https://arxiv.org/pdf/2401.04521.pdf

SUPRATECH |Preprint

**HyperNova Bridgeless Service**

Raghavendra Ramesh and Aniket Kate

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com

The official whitepaper of Supra.

FIRST PUBLISHED: October 27, 2023 | Share https://supra.com/documents/Supra-HyperNova-Whitepaper.pdf

SUPRATECH |Publication

**FlexiRand: Output Private (Distributed) VRFs and Application to Blockchains**

Aniket Kate, Pratyay Mukherjee, Easwar V. Mangipudi and Siva Maradana

30th ACM Conference on Computer and Communications Security (CCS), 2023

LATEST VERSION: JULY 28, 2023 | Share https://supra.com/documents/Supra-FlexiRand-PVRF.pdf

SUPRATECH |Publication

**Moonshot: Optimistic Proposal for Blockchain-Based State Machine Replication**

Isaac Doidge, Raghavendra Ramesh, Joshua Tobkin and Nibesh Shrestha

54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2024

LATEST VERSION: JULY 12, 2023 | Share https://supra.com/documents/Moonshot-Whitepaper.pdf

SUPRATECH |Publication

**Non-interactive VSS using Class Groups and Application to DKG**

Aniket Kate, Easwar Vivek Mangipudi, Pratyay Mukherjee, Hamza Saleem, Sri Aravinda Krishnan Thyagarajan

31th ACM Conference on Computer and Communications Security (CCS), 2024

LATEST VERSION: MAY 24, 2022 | Share https://eprint.iacr.org/2023/451.pdf

SUPRATECH |Publication

**DORA: Distributed Oracle Agreement with Simple Majority**

Saurabh Joshi, Aniket Kate, Joshua Tobkin and David Yang

43rd IEEE International Conference on Distributed Computing Systems (ICDCS), 2023

LATEST VERSION: MAY 12, 2023 | Share https://arxiv.org/pdf/2305.03903.pdf

SUPRATECH |Preprint

**Dynamic Function Market Maker**

Arman Abgaryan and Utkarsh Sharma

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Português
Indonesia
Türkçe

Archived copy · cryp2nova.com

LATEST VERSION: FEBRUARY 25, 2023 | Share https://arxiv.org/pdf/2307.13624

The official wallet of Supra.



Archived copy · cryp2nova.com

The official wallet of Supra.

EN

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Privacy • Terms of Use • Website Data Usage & Cookies • Bug Disclosure • Biometric Information Privacy Policy

©2026 Supra | Entropy Foundation (Switzerland: CHE.383.364.961). All Rights Reserved

English
简体中文
繁體中文
한국어
Tiếng Việt
español
Русский язык
Indonesia
Türkçe

Archived copy · cryp2nova.com