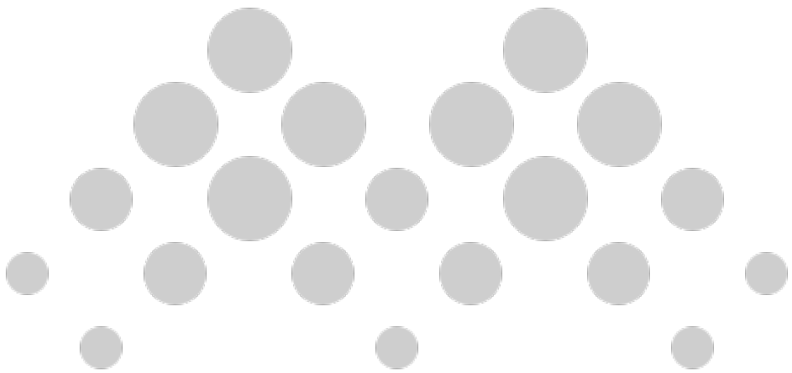
MATH Whitepaper

IN MATH WE TRUST



Introduction

MATH is a multi-chain and cross-chain blockchain assets hub, and its products include MathWallet (supporting over one hundred blockchains including BTC, ETH, Polkadot, Cosmos, Filecoin, Solana, BNBChain, etc and 3 million users), MathVault, MathDAppStore, MathStaking, MathNFT, MathVerse, etc. Our investors include Fenbushi Capital, Binance Labs, FundamentalLabs, Multicoin Capital, NGC Ventures, Amber Group, 6Eagle Capital. Visit mathwallet.org for more information.

Building upon the existing user base of over 3 million users and connection with more than 160 public blockchains in the MATH ecosystem, we are proposing a modular L2 blockchain architecture and will construct MathChain based on this framework.

Overview

MathChain is an EVM-based L2 SmartWallet AppChain for massive adoption, go-to-market, and inclusive blockchain applications.

To reach this goal, we saw problems in below 4 areas at the current stage:

1. Security Cost

   The annual cost of securing major chains (e.g., Cosmos, Tezos, and EOS) is in the tens of millions of USD per year, with Ethereum and Bitcoin in the billions.

2. Performance

   If we need a permissionless environment like Ethereum, we must endure 12 TPS and a very high gas fee.

3. Privacy

   The distributed aspect of a blockchain means that each full node that processes transactions and builds the blockchain has access to the blockchain transaction data. The blockchain is publicly available in a cryptocurrency like Bitcoin, and every transaction can be traced back to the first Genesis block.

4. Account

   We need the evolution of crypto wallets so that it is not for whales to store crypto only but for more and more users to use them daily.

Because of these problems, we saw more off-chain & centralized systems than on-chain systems when the application needed a better user experience.

The future of blockchain is for massive adoption. And for MathChain, here are the solutions:

1. Share Security

   Leveraging the L1 blockchain share security mechanism, the cost of security in MathChain would be a complete three to five orders of magnitude less and yet would provide fast, arbitrary, trust-free message passing between the host chains, a revolutionary addition. Most important, it connects MathChain to the L1 Relay Chain and obtains the same security as the Polkadot Relay Chain, thus ensuring the safety of assets on MathChain.

2. Parachain

The underlying mechanisms of Substrate and Polkadot can provide sufficient transaction speed and low cost. MathChain will implement a fee market to have more predictable transaction fees.

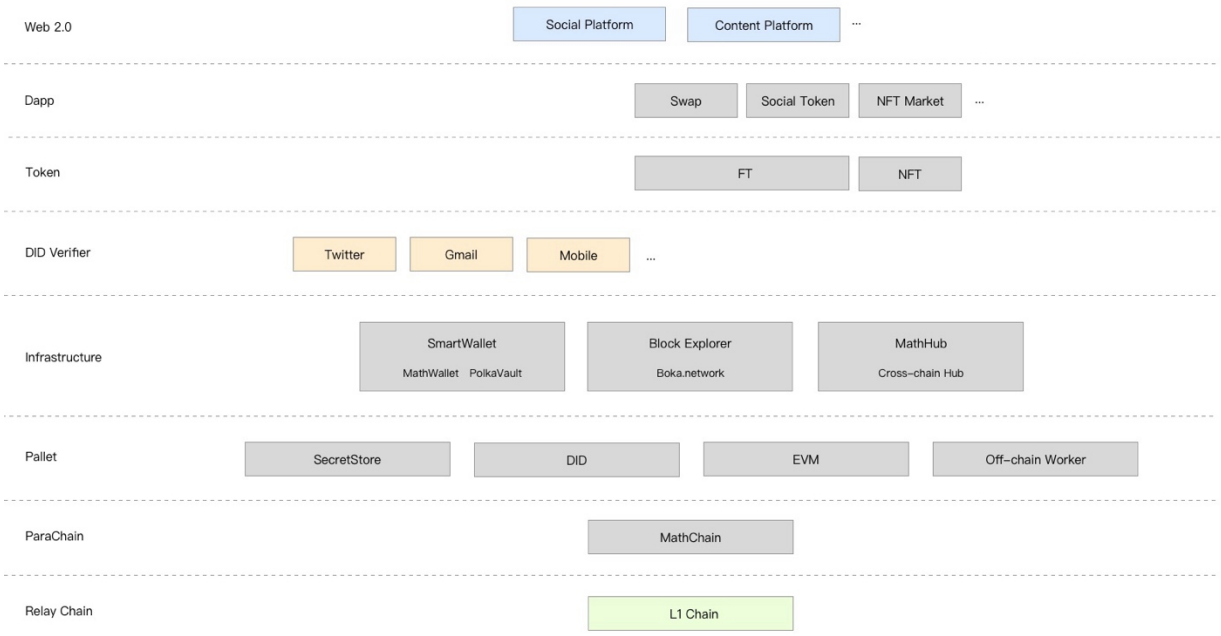
3. SecretStore

   The SecretStore module on MathChain makes all the information you want to send to someone even more private. It can be leveraged by an on-chain transaction or an off-chain Filecoin storage request.

4. Smart Wallet combines SecretStore, Off-chain Worker, and DID; MathChain can build universal interchain accounts with easy recovery without a paper backup. It will bring the user's Web 2.0 social media account relation to Web 3.0. It will not only store assets but data as well.

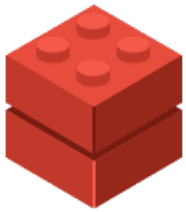
The goal is to provide account / performance / infrastructure readiness and allow Web 2.0 platforms to connect easily to the Web 3.0 ecosystem without sacrificing user experience.

Architecture



Modules

Basic modules are the LEGOs for MathChain applications.



SecretStore

Secret Store allows users to store on the blockchain a fragmented ECDSA key, which retrievals are controlled by a SmartContract. All of this, running under a Threshold System makes nodes unable to read the keys on their own and makes your documents or secrets totally safe.

It will bring privacy capability to MathChain.

DID

A Decentralized Identifier (DID) is a new type of identifier that is globally unique, resolvable with high availability, and cryptographically verifiable.

MathChain DID is also the account service associated with account public keys and can connect to service endpoints for establishing secure communication channels. It allows the creation of a unique account name and can connect with the user's social platform account.

EVM

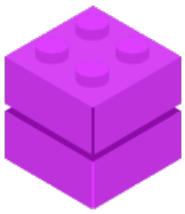
This is the Substrate's Ethereum compatibility module. It allows MathChain to run unmodified Ethereum dapps. Run a normal web3 application via the compatibility layer, using local nodes, where an extra bridge binary is acceptable. It is able to import state from Ethereum mainnet.

It also contains the basic tools to support EVM including block explorer, web3js support wallet etc.

It will power MathChain to be the EVM compatible layer 2 blockchain with high performance. And combine with small wallet, dappstore, datastore, it will bring more interesting applications to MathChain.

Off-chain Worker

Off-chain Workers allows the processes that are too intensive or data that's too massive to be handled by specialized nodes on the network, all while storing the code for how to do the work on-chain to ensure participants are automatically kept up to date with the latest logic that their chain dictates.



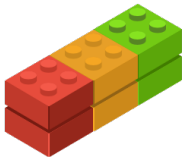
XCMP

XCMP (Cross-chain Message Passing) is the mechanism to route messages between parachains and parathreads. It supports a smart contract that exists on parachain A will route a message to parachain B in which another smart contract is called that makes a transfer of some assets within that chain.

It will make MathChain able to do cross-parachain message exchange.

Applications

Next we start to build decentralized apps with these LOGOs on MathChain.



SecretStore + Off-chain Worker + DID = MathSmartChainWallet

MathWallet has supported more than 60 public chains, with over a million users so far, however, we have never stopped thinking about the future of the blockchain world, and the most important issue is how to serve the mainstream users.

Smart Wallet is an area that MATH has constantly been researching, and we saw the value of Smart Wallet in lowering the barriers for new users to participate, some products have done great in the smart wallet field, such as Argent, and Dapper.

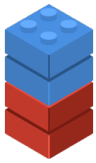
But we also saw some of the limitations of Smart Wallet today:

1. Account creation costs are high because it needs to create the mainnet contract for each new user.

2. Smart contract transaction has limitation in some scenarios, such as the exchange blocks the smart contract deposit, etc.
3. Difficulty in upgrading smart contracts.

Thus, we are introducing a new generation of 'Smart Chain Wallet', which will address those problems by moving the logic of smart contracts into MathChain.

In the design, distributed key management is powered by SecretStore. Social account verification is handled by Off-chain Workers in a decentralized way. And Combined with DID, smart wallet is able to support namespace, spending limitation, social account recovery and lock/unlock functions.



SecretStore + Filecoin = SecretVault

SecretVault is the personal data vault for all users.

SecretStore module on MathChain allows us to save the encrypted data on the Filecoin storage service without any worries about our privacy. It moves computation and data storage off-chain while keeping the data ownership and permission control on-chain.

We will also be able to share data with others through the MathChain ecosystem. Data that no one will be able to read without your permission (even node owners, which is pretty important and was the handicap we had on previous schemes).

This scheme is GDPR friendly so that no personal data or sensitive data is ever deployed/uploaded to the blockchain; the user who encrypted it is the only one who has the right to share the document and the key session with others. The permissions are controlled on MathChain.

Since MathWallet is also the first batch of Filecoin Notaries, we will partner with the best Filecoin storage service provider and connect the L1 blockchain and Filecoin.

A MathHub bridge will be built between MathChain and Filecoin; users only need to pay MATH, and they will get storage space in Filecoin for private data. MathHub will handle the cross-chain token swap, etc.

This will also make the data exchange market possible on MathChain in the future.

Eventually, SecretVault will be the data bank for everyone and take the control of personal data back to the user's own hands.

SecretStore + MathDappStore = MathSecretStore

MathDappStore is the place to satisfy all the decentralized app needs and the entry for all DApp users. It lists 5000+ open-source dApps for 200+ blockchains in 20 categories.

Most of the DApps in MathDappStore are open-source, which brings trust, but it also causes the fork issue. And currently, this issue cannot be solved based on the current dappstore model.

Encrypt SmartContracts and create MarketPlaces with dApps, giving developers the assurance that nobody will be able to read or copy their code. Only the security auditing team will be granted the decoded access and publish their auditing results.

MathSecretStore will also become the world's first fully decentralized appstore, in which MATH token will be used as a governance token for rating, listing, indexing, etc.

This will make those with dApp-designed businesses much more viable than apps in the Google Play Store and Apple App Store.

EVM + Off-chain Worker = MathHub

Currently, there are normally 2 methods: PoA bridge and HTLC.

They have some limits:

1. Rely on a set of authorities.

2. Need multiple pools for different bridges.
3. Must go through layer-1 network

For MathHub:

1. A bridge token is an intermediary asset that leverages Off-chain Worker mechanism to quickly move between different chains.
2. Wrapped cross-chain tokens and bridge tokens can be swapped using AMM DEX on each chain.
3. Incentive market maker to rebalance liquidity across the network.

MathHub + Rollup = MathHub Rollup to Rollup Bridge

A rollup is a layer-2 solution that has become one of the cornerstones of the layer-1 scaling roadmap like Ethereum. Each rollup provides an execution environment that can process transactions similarly to layer-1 itself but at a fraction of the cost.

There are 2 requests we found in the cross-rollup situation:

1. The duration of exits from rollups is very long
2. There are no cross-rollup protocols

But by leveraging MathHub's cross-chain function, we can:

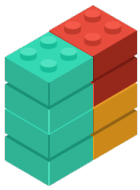
1. Allow tokens to be quickly and easily sent from one roll up to the next
2. Enable fast exits from rollups
3. Support cross-rollup contract calls eventually

MathHub + EVM + MathVault v1 = MathVault v2

MathVault (VPoS) is a new kind of mining pool that rewards you with both mining rewards and MATH tokens, which TVL has exceeded $150M.

MathVault v2 will be an intelligent staking aggregator and yield engine, like Yearn, for cross-chain assets and DeFi protocols.

MathHub & XCMP provide the cross-chain capability. Based on EVM, MathVault v2 can support on-chain strategies based on smart contracts and bring the highest APR for users.



MathHub + EVM + SecretStore = DeFi with Privacy

Blockchain is a decentralized network of nodes with constant data exchange regarding the modifications in their state or mempool. As the transaction order is not assigned until the finalization state, any decentralized exchange based on Blockchain will be prone to frontrunning.

Front-running happens because bots can bid a slightly higher gas price on a transaction, incentivizing miners to place earlier in the order when constructing the block. The higher-paying transactions are executed first. Thus, if two transactions making a profit from the same contract call are placed in the same block, only the first takes the profit.

Evolve the permissions SmartContract to create a private-transactions ecosystem, which most of the blockchains want to do, and with EVM + SecretStore, MathChain will be able to do that. At the same time, MathHub will be able to finish the interoperability with contracts on the other chains.

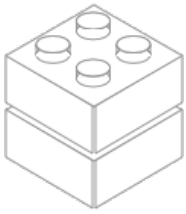
MathSmartWallet + DID + EVM = MathPay

MathPay is the Blockchain Micro-payment system.

There are still a lot of people who do not have bank accounts in this world. They can use a social account to create the DID in MathSmartWallet. Then, they can start to use ERC20 standard tokens for payment in real life.

Combined with DeFi applications, they can do lending and swap. They can join yield farming to increase their assets and buy blockchain-based insurance programs.

Micro-payment will also bring new business models in real life; for example, content creators can get paid with a very small amount of tokens when their content gets viewed, which will replace their current advertising model. The small amount can have 18 decimals, which is not possible in the current digital payment system.



MathDappFactory + Your Idea = ?

MathDappFactory provides developers with great tools that make developing exchanges, games, and DApps snap.

Developers can leverage MathDappFactory to build their own ideas without a long learning curve. They can also propose a MathChain treasury request to create public good on MathChain and will be rewarded with MATH token if it passes the governance.

We gladly invite the developer community to join us on this journey.

Verifier

Verifier provides different 3rd party verification services to the SecretStore.

Verifiers can have different verification methods, decentralized levels, and costs.

For example, the TwitterID verifier will connect to Twitter API and verify if the address controls the Twitter account and provides access to a specific secret key in SecretStore.

Another verifier example is the NFT verifier, which can verify if the address contains a specific NFT token and then provide access to a specific secret key in SecretStore.

Verifier SecretStore access can be switched to another verifier if the verifier retires.

Tokenomics

MATH Token

An initial total limit of 200M MATH will be created. MATH will run natively on Ethereum as an ERC20 token initially and will migrate to MathChain after launch.

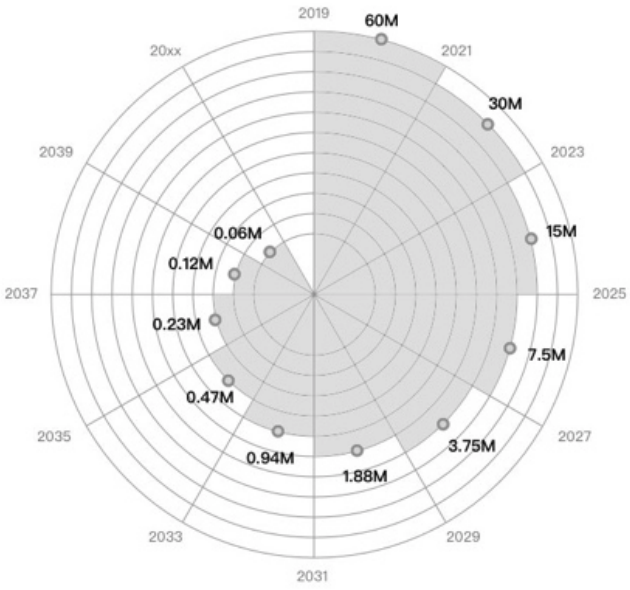
Professional investor includes Fenbushi Capital, Alameda Research, Binance Labs, FundamentalLabs, Multicoin Capital, NGC Ventures, 6Eagle Capital, and Amber Group.

MATH VPoS Mining Pool	60%	120M
Professional Investor	30%	60M
Lockdrop Investor	10%	20M

MATH Token Farming

Math farming power is based on the market value of BTC, ETH, DOT, MATH, and other assets that users deposit in the MathVault Mining Pool. 10% of mined MATH tokens will go into MathChain Treasury, and the rest 90% will be sent to mined users. Treasury will be controlled by MathChain governance. The mining pool of MATH halved every two years.

MATH token farming started on 2019-09-26 12:00:00 Singapore Time, details on http://explorer.mathwallet.org



MATH Token Annual Issuance

Issuance will NOT start until the MATH Chain mainnet launch. Max annual issuance will be determined by the average monthly staking rate of MATH. MATH tokens will be issued to reward MathChain stakers and node operators.

Staking Rate	Max Annual Issuance
<5%	20M
5%-20%	10M
20%-50%	2M
50%-100%	1M

MATH Token Burn

All MATH transaction fees & cross-chain message fees will be burned.

MathChain implements a fee market to have more predictable transaction fees. With this method, the base transaction fees are burned. Unlike Bitcoin/Ethereum, the fee will not need to reward miners but will be burned to increase the value.

MATH Token Usage

1. Transaction fee
2. Cross-chain message fee
3. Participation governance
4. MathWallet service fee

Governance

MathChain has an on-chain democracy system. Users and a democratically elected council can submit referendum proposals voted on by token holders. This user-driven governance system allows MathChain to enact runtime upgrades much more efficiently and with a much-reduced risk of network split compared with hard-fork-based governance systems.

The same system also allows upgrading the consensus, including mining and difficulty adjustment algorithms.

A democratic governance system allows MathChain to build a public-good treasury system, with token holders having the final say on how funds are spent. Treasury taxation is fair and, at the same time, voluntary, reducing the risk of centralization and misuse.

Ecosystem

MathWallet has supported and partnership with more than 160 blockchains:

Mainstream

- ✓ Bitcoin
- ✓ Filecoin
- ✓ Flow
- ✓ Sui
- ✓ Conflux
- ✓ VeChain
- ✓ EVM
- ✓ EOS FORCE
- ✓ Enumivo
- ✓ NEO
- ✓ WORBLI
- ✓ Solana Testnet
- ✓ Solana
- ✓ Arweave
- ✓ TRON
- ✓ EOS
- ✓ Nervos
- ✓ Harmony
- ✓ TON
- ✓ YAS
- ✓ BOS
- ✓ Nebulas
- ✓ Wax
- ✓ APTOS
- ✓ Tezos
- ✓ Near
- ✓ BNB Beacon Chain
- ✓ Ontology
- ✓ Substrate
- ✓ Zilliqa
- ✓ FIBOS
- ✓ TelosEOS
- ✓ Ethersocial
- ✓ NFT

EVM

- ✓ Ethereum
- ✓ Polygon
- ✓ Arbitrum Nova
- ✓ Moonriver
- ✓ Heco
- ✓ GnosisChain
- ✓ OasisNetwork
- ✓ Rootstock
- ✓ Harmony EVM
- ✓ EthereumPoW
- ✓ GateChain
- ✓ smartBCH
- ✓ Swimmer
- ✓ XDC
- ✓ Flare
- ✓ Conflux eSpace
- ✓ Polygon zkEVM
- ✓ Neon EVM
- ✓ Kava EVM
- ✓ Mantle
- ✓ CoinEx Smart Chain
- ✓ ApeChain
- ✓ IoTeX
- ✓ BAS Testnet
- ✓ BNBChain
- ✓ Arbitrum One
- ✓ Moonbeam
- ✓ Fantom
- ✓ Evmos
- ✓ Cronos
- ✓ Syscoin
- ✓ Klaytn
- ✓ AstarEVM
- ✓ EthereumFair
- ✓ KCC
- ✓ Fuse
- ✓ Cube Chain
- ✓ Bitgert
- ✓ Canto
- ✓ FVM
- ✓ EOS EVM
- ✓ ZetaChain Testnet
- ✓ Zora
- ✓ Aurora
- ✓ Palm
- ✓ TomoChain
- ✓ opBNB Testnet
- ✓ Base Goerli
- ✓ Base
- ✓ OP Mainnet
- ✓ OKXChain
- ✓ Avalanche
- ✓ Celo
- ✓ Metis
- ✓ PlatON
- ✓ HooSmartChain
- ✓ ShidenEVM
- ✓ zkSync Era
- ✓ Godwoken
- ✓ MilkomedaCardano
- ✓ TelosEVM
- ✓ HumanodeEVM
- ✓ ENULS
- ✓ Scroll Alpha
- ✓ Core
- ✓ Linea
- ✓ Scroll Sepolia
- ✓ Songbird
- ✓ Boba
- ✓ Ethereum Classic
- ✓ BSC Testnet

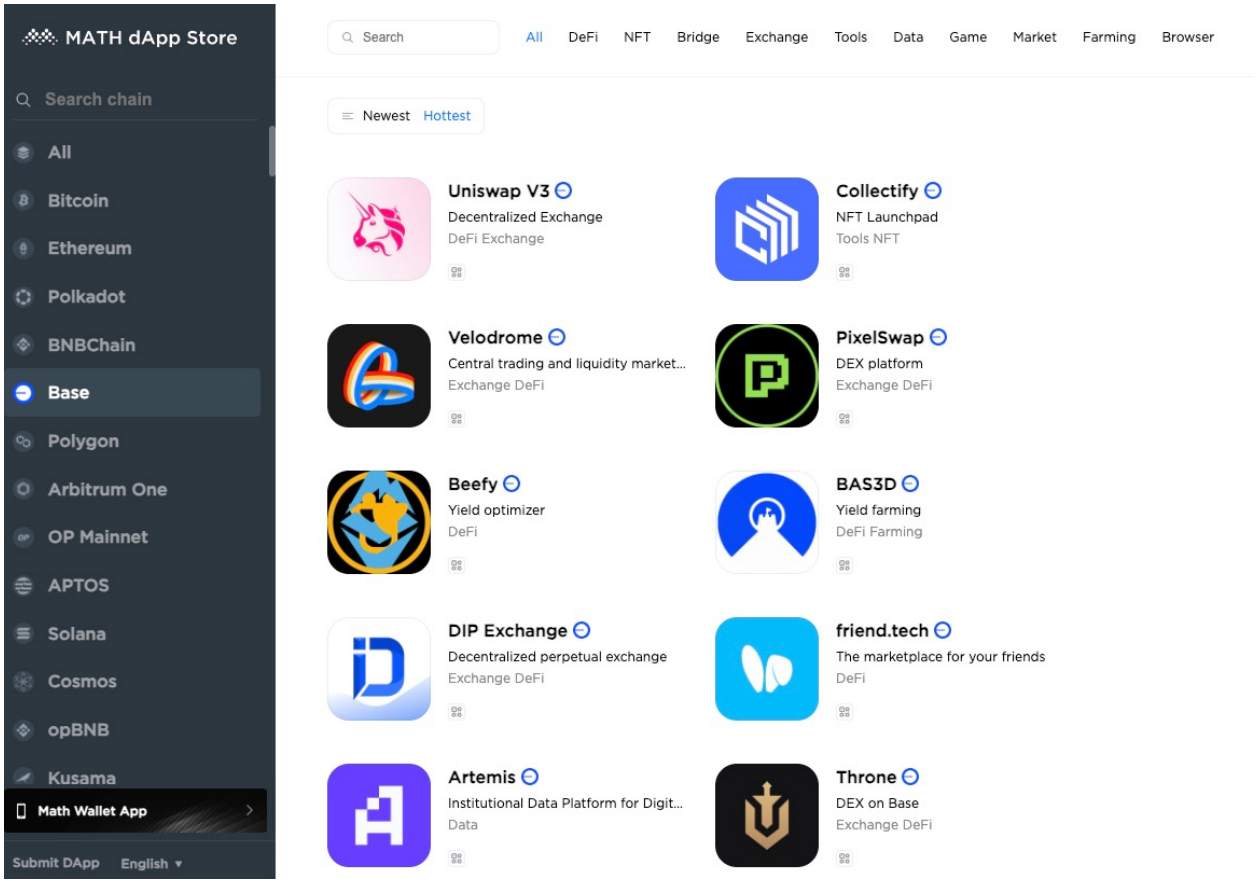
Substrate

- ✓ Polkadot
- ✓ Acala
- ✓ Bifrost Polkadot
- ✓ ChainX
- ✓ Clover
- ✓ Shiden
- ✓ Basilisk
- ✓ Statemint
- ✓ OriginTrail Parachain
- ✓ Humanode
- ✓ Kulupu
- ✓ Subsocial Parachain
- ✓ Darwinia Crab
- ✓ Kusama
- ✓ Karura
- ✓ Khala
- ✓ CRUST
- ✓ Darwinia
- ✓ Calamari
- ✓ Neatcoin
- ✓ Efinity
- ✓ Phala
- ✓ Edgeware
- ✓ Stafi
- ✓ Subsocial Solochain
- ✓ DBC Mainnet
- ✓ Statemine
- ✓ Bifrost Kusama
- ✓ Parallel
- ✓ KintsugiBTC
- ✓ Astar
- ✓ KILT Spiritnet
- ✓ Quartz
- ✓ Composable Finance
- ✓ UNIQUE
- ✓ Equilibrium
- ✓ Centrifuge
- ✓ Sora

CosmosSDK

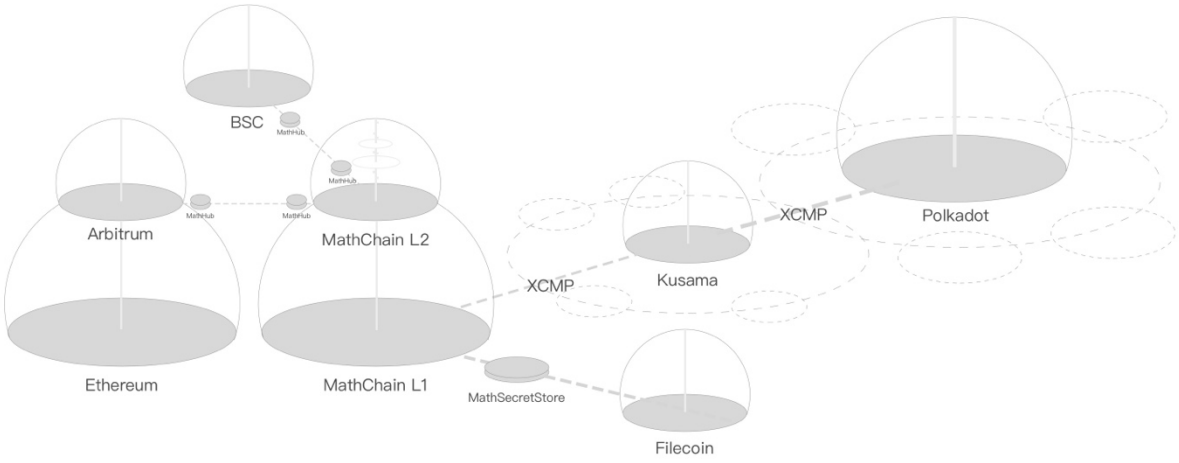
- ✓ Cosmos
- ✓ KAVA
- ✓ Osmosis
- ✓ Certik
- ✓ Persistence
- ✓ IXO
- ✓ Sommelier
- ✓ Injective
- ✓ Archway Constantine
- ✓ IRISnet
- ✓ THORChain
- ✓ Akash
- ✓ Sentinel
- ✓ Crypto.org
- ✓ Juno
- ✓ Gravity Bridge
- ✓ Noble
- ✓ SEI atlantic 2
- ✓ Secret Network
- ✓ Band Protocol
- ✓ Starname
- ✓ Regen
- ✓ Axelar
- ✓ Stargaze
- ✓ Umee
- ✓ Sei

Math dApp Store has listed and partnered with more than 5,000 dApps on 160+ blockchains.


MATH dApp Store
Search chain
All
Bitcoin
Ethereum
Polkadot
BNBChain
Base
Polygon
Arbitrum One
OP Mainnet
APTOS
Solana
Cosmos
opBNB
Kusama
Math Wallet App
Submit DApp
English
Search
All
DeFi
NFT
Bridge
Exchange
Tools
Data
Game
Market
Farming
Browser
Newest
Hottest
Uniswap V3
Decentralized Exchange
DeFi Exchange
Collectify
NFT Launchpad
Tools NFT
Velodrome
Central trading and liquidity market...
Exchange DeFi
PixelSwap
DEX platform
Exchange DeFi
Beefy
Yield optimizer
DeFi
BAS3D
Yield farming
DeFi Farming
DIP Exchange
Decentralized perpetual exchange
Exchange DeFi
friend.tech
The marketplace for your friends
DeFi
Artemis
Institutional Data Platform for Digit...
Data
Throne
DEX on Base
Exchange DeFi

Road Ahead

Eventually, MathChain will be a decentralized permissionless L2 that allows easy interoperability with Polkadot / Ethereum / BSC / Filecoin / Rollups / EVM side chains and focus on massive adoption / go-to-market / inclusive blockchain applications.



Partners


FENBUSHI
CAPITAL
BINANCE
LABS
Fundamental
Labs
Multicoin Capital
NGC
CoinGecko
DeBank
Your DeFi Wallet
NODEREAL
TheGraph
blocknative

Resources

https://mathwallet.org

https://twitter.com/MathWallet

https://github.com/mathwallet