MathChain WhitePaper

MathChain: Layer 2 blockchain based on Substrate

Version: v0.9.3

Overview

MathChain is a layer 2 blockchain based on Substrate 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 need to endure 12 TPS and very high gas fee.
3. Privacy
   The distributed aspect of a blockchain means that each full node that processes transactions and builds the blockchain necessarily has access to the blockchain transaction data itself. In a cryptocurrency like bitcoin, this means that the blockchain is publicly available and every transaction can be traced back to the first genesis block.
4. Wallet

   We need evolution of crypto wallet so that it is not for whales store crypto only, but for more and more users to use them in daily life.

We believe the future of layer 2 blockchain is for massive adoption. And for MathChain, here are the solutions:

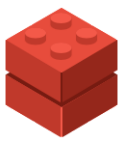
1. Share Security
   Leverage the polkadot share security mechanism, the cost of security in MathChain would be a full three to five orders of magnitude less, and yet

would provide fast, arbitrary, trust-free message passing between the host chains, a revolutionary addition. And most important, being connect MathChain to the Polkadot Relay Chain, and obtain 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 fee market, which is a method to have more predictable transaction fees.
3. SecretStore
   The SecretStore module on MathChain which makes even more private all the information you want to send to someone. It can be leveraged by both an on-chain transaction or a off-chain Filecoin storage request.
4. Smart Wallet
   Combine SecretStore, Off-chain Worker and DID together, MathChain is able to build the universal interchain accounts with easily recover without a paper backup. It will bring user's web 2.0 social media account relation to web 3.0.

Modules

Basic modules are the LEGOs for MathChain applications.



SecretStore

Secret Store allows user to store on the blockchain a fragmented ECDSA key which retrievals are controlled by a SmartContract. All of this, running under a Threshold System that makes nodes unable to read the keys on it’s 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, resolveable with high availability, and cryptographically verifiable.

MathChain DID is associated with account public keys, and can connect to service endpoints, for establishing secure communication channels.

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.

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.

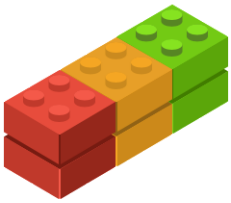
XCMP

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.

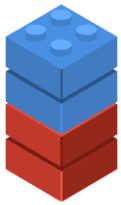
Smart Wallet is an area that MATH has always been researching, and we saw the value of Smart Wallet in lowering the barriers for new users to participate, there are some products that have done great in smart wallet field, such as Argent, Dapper, and MYKEY.

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

1. Account creation costs are high, because it need 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 for upgrading smart contract.

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

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



SecretStore + Filecoin = PolkaVault

PolkaVault is the personal data vault for all users.

SecretStore module on MathChain allows us save the encrypted data on 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 able to share data with others through MathChain ecosystem. Data that no one will be able to read it without your permission (even node owners which is pretty important and was the handicap we had on previous schemes).

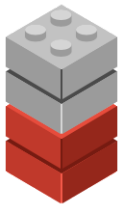
This scheme is GDPR friendly in order that no personal data or sensitive data is never deployed/uploaded to the blockchain, the user who encrypted it is the only one ho has the rights to share the document and the key session with others. The permissions are controlled on MathChain.

Since MathWallet is also the first batch of Filecoin Notaries, we will partnership with the best Filecoin storage service provider and bring Polkadot and Filecoin connected together.

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 data exchange market possible on MathChain in future.

Eventually, PolkaVault will be the data bank for everyone, and take the control of personal data back to 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 3000+ open-source dApps for 65 bockchains in 20 categories.

Most of the DApps in MathDappStore are open-source, which brings trust, but it also cause 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 grant the decode access and publish their auditing results.

MathSecretStore will also become the world's first fully decentralized appstore, which MATH token will be used as 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

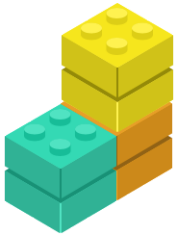
Currently there are normally 2 methods: PoA bridge and HTLC.

They have some limits:

1. Rely on a set of authorities.
2. Need multiple pools for different bridges.
3. Must go throught layer-1 network

For MathHub:

1. Bridge token as an intermediary asset which leverage Off-chain Worker mechanism to quickly move between different chains.
2. Wrapped cross-chain token and bridge token is able to swap use AMM DEX on each chain.
3. Incentive market maker to rebalancing of liquidity across the network.



MathHub + Rollup = MathHub Rollup to Rollup Bridge

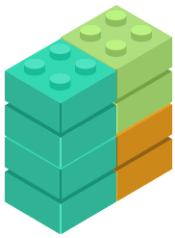
A rollup is a type of layer-2 solution that has become one of the cornerstones of the layer-1 scaling roadmap like Ethereum. Each rollup provides an execution environment that can process transactions in a similar way to layer-1 itself but at a fraction of the cost.

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

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

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

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

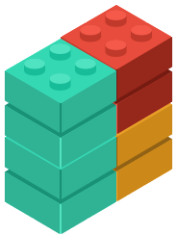


MathHub + EVM + MathVPoS v1 = MathVPoS v2

Virtual Proof of Stake (VPoS) is a new kind of mining pool that rewards you with both mining reward and MATH tokens which TVL has exceed $150M.

MathVPoS v2 will be a smart staking aggregator and yield engine, like Yearn, for cross-chain assets and DeFi protocols.

MathHub & XCMP provides the cross-chain capability. Based on EVM, MathVPoS v2 is able to support on-chain strategies based on smart contract and bring the highest APR for users.

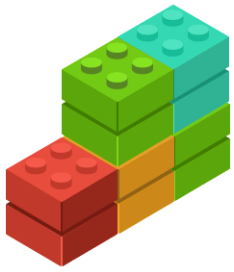


MathHub + EVM + SecretStore = DeFi with Privacy

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 are able to 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 permissioning SmartContract in order to create a private-transactions ecosystem, which is something that 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 interoperaibility with contracts on the other chains.



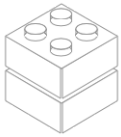
MathSmartWallet + DID + EVM = MathPay

MathPay is the Blockchain Micro-payment system.

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

Combine with DeFi applications, they can do lending and swap. They can join yield farming to increase they assets and buy blockchain based insurance program.

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



MathDappFactory + Your Idea = ?

MathDappFactory provides developer with great tools that make developing exchanges, games, and other DApps a 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.

Tokenomics

MATH Token

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

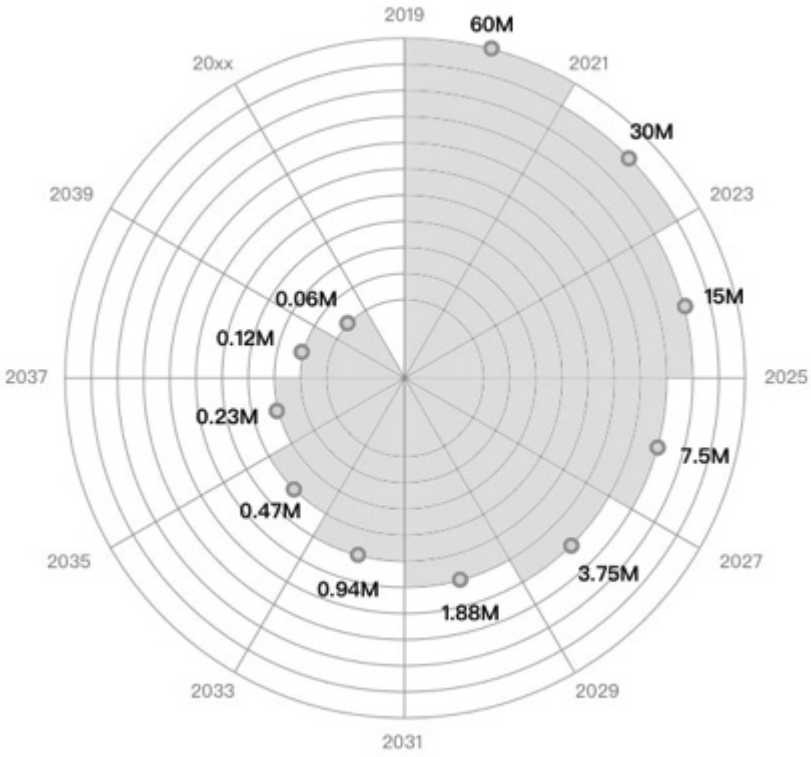
Professional investor includes Fenbushi Capital, Alameda Research, Binance Labs, FundamentalLabs, Multicoin Capital, NGC Ventures, 6Eagle Capital, Amber Group.

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

MATH Token Farming

Math farming power based on the market value of BTC, ETH, DOT, MATH and other assets that user deposit in the MATH VPoS Mining Pool.
10% mined MATH tokens will go into MathChain Treasury, rest 90% will send to mined users. Treasury will be controlled by MathChain governance.
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 MATH Chain mainnet launch.
Max annual issuance will be determined by average monthly staking rate of MATH.
Issuance MATH token will be used to reward parachain auction participants and parachain/parathread collators to acquire mainnet security.

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

MATH Token Burn

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

MathChain implements fee market, which is a method 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 itself.

MATH Token Usage

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

Governance

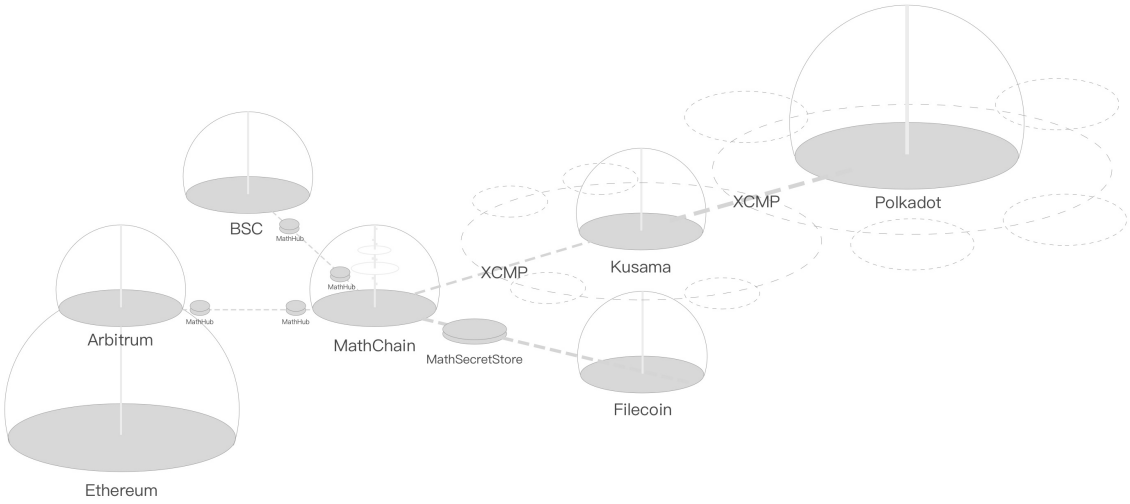
MathChain has an on-chain democracy system. Users and a democratically elected council can submit referendum proposals, which are voted by coin holders. This user-driven governance system allows MathChain to enact runtime upgrade much more easily, and with much reduced risk of network split, compared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

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

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

Road Ahead

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



Live MathChain Roadmap:

https://www.notion.so/mathchain/f2abd4d6d4c54ee3a6fafd7cbe37b0fa?v=5ae6e992dd004c96941f0727697ae928

Resources

https://mathchain.org

https://twitter.com/MathChainOrg

https://mathwallet.org

https://twitter.com/MathWallet

https://github.com/mathwallet