

Matic Network

Scalable, secure and instant blockchain transactions using sidechains, while ensuring asset security using the Plasma framework and a decentralized network of Proof-of-Stake (PoS) validators.

Decentralized Apps are making huge progress but the current blockchain ecosystem is not prepared to scale as per the demand. Slow block confirmations, block size limitations and computations — in smart contract based blockchains — need to be solved before we target mass adoption by mainstream users. And most importantly, it needs an awesome user experience.

With Matic Network, we aim to solve this by having Plasma-based side-chains on top of Ethereum for high scalability and secure transactions.

One of the key pillars of Matic Network's ideology is user experience which is very poor for Blockchain applications as of now.

Matic Team has already built high-quality user experience Mobile/Web browser libraries (like WalletConnect) and tools such as Dagger which will enable businesses to create real-world end-user applications at large scale.

What is Matic Network?

Matic provides scalable, secure and instant transactions using sidechains based on an adapted implementation of Plasma framework for asset security and a decentralized network of Proof-of-Stake (PoS) validators. In short, it allows anyone to create scalable DApps while ensuring a superior user experience in a secure and decentralized manner. It has a working implementation for Ethereum on Ropsten Testnet. Matic intends to support other blockchains in the future which will enable it to provide interoperability features alongside offering scalability to existing public blockchains.

Medium blog on what is Matic Network and tech architecture:

<https://medium.com/matic-network/what-is-matic-network-466a2c493ae1>

You can also read our whitepaper at <https://whitepaper.matic.network>

Key things Matic wants to do:

- Solve scalability by providing Layer 2 solutions
- Application platform for DApp developers on Matic (developer experience like Stripe for DApps)
- Provide assets interoperability via DEXs
- Better UX/UI for mass adoption while having better security and scalability

Matic intends to provide Matic wallet, payment APIs and SDKs, products, and other enabling solutions that will allow developers to design, implement and migrate DApps built on base platforms like Ethereum. Matic will also allow cross-chain transfers like BTC (using pegging) - that way, anyone can trade any currencies on Matic based DEX.

User flow for crypto assets on Matic

- User deposits crypto assets in Matic contract on the mainchain (currently implemented with Ethereum blockchain only)
- Once deposited, tokens get confirmed on the mainchain, the corresponding tokens will get reflected on the Matic chain.
- The user can now transfer tokens to anyone they want instantly with negligible fees. Matic chain has faster blocks (approximately 1 second or less). That way, the transfer will be done almost instantly.
- Once a user is ready, they can withdraw remaining tokens from the mainchain by establishing proof of remaining tokens on Root contract (contract deployed on Ethereum chain)

Remember any crypto assets can be represented as ERC20 or ERC721 tokens on Matic chain. That way, the same method will work for any fungible or non-fungible crypto assets like Bitcoin, crypto kitties and other tokens/NFTs.

Tech architecture

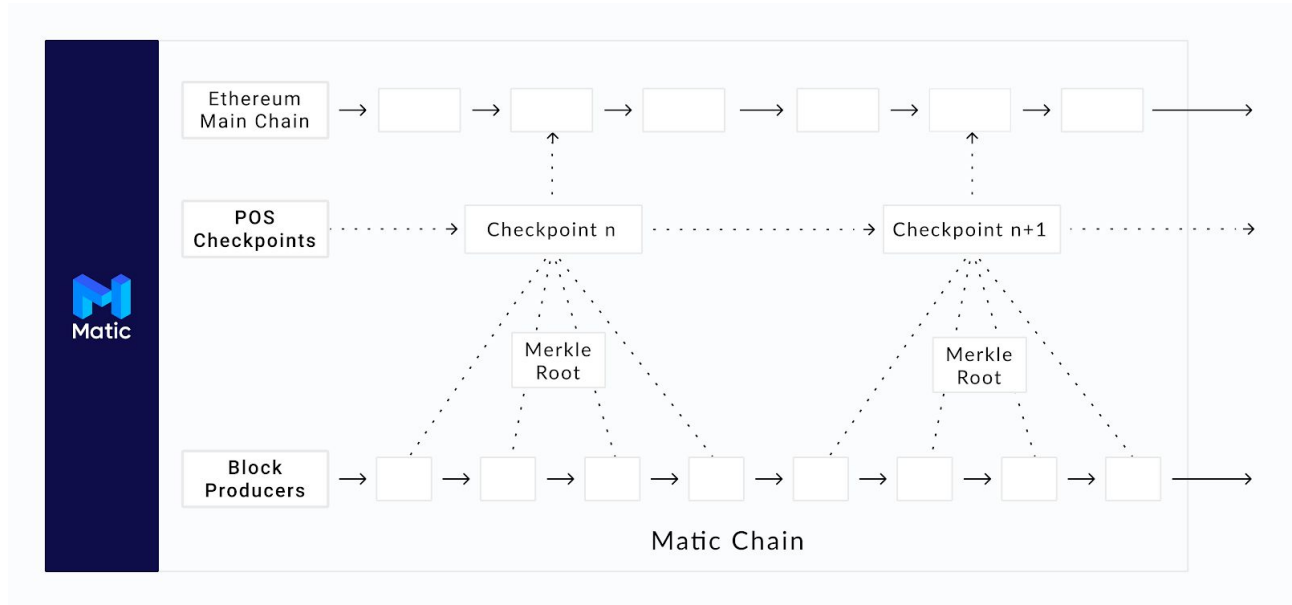
Matic ecosystem will have the following actors:

- *End Users*
- *DApp developers*: Developers will be the businesses who would be using Matic to scale their applications and provide a better UI/UX to their end users.
- *Stakers*: Stakers need to deposit/stake tokens to qualify and play a very important role in the Matic Network. They validate the transactions and propose checkpoints on the mainchain using PoS consensus mechanism with a $\frac{2}{3}$ majority. They also choose Block Producers amongst themselves, who satisfy certain criteria, to produce blocks on the sidechains.
- *Block Producers*: Block producers are chosen by Stakers and enable faster block generation times. They have to provide a significant stake to be nominated.

Matic uses a dual strategy of Proof of Stake at the Checkpointing layer and the Block Producer layer to achieve the faster block times while ensuring the high degree of decentralization by achieving finality on the mainchain using checkpoints and fraud proofs (security).

Anyone can stake their Matic tokens on root contract to become a Staker in the PoS checkpointing layer. This provides a high degree decentralized base layer for Matic chain and ensures liveness of chain.

At the Matic block layer, we have block producers selected by PoS Stakers on the base layer who will be creating the Blocks. To achieve faster block generation times these block producers will be few in number. This layer will achieve < 2-second block generation times at extremely low to negligible transaction fees.



This diagram represents how Matic works on top of Ethereum

To enhance the security of the transactions, Matic also provides Fraud Proofs on the mainchain. This mechanism enables any individual on the mainchain to submit the details of the transactions which he/she thinks is fraudulent. If the challenge is successful, the stakes of the parties involved in the fraud are slashed and the challenger receives the slashed funds as an incentive to detect the fraud. This can be considered an ever running high reward bounty program for any parties who want to investigate the veracity of the transactions on the Matic Network.

You can also read our whitepaper at <https://whitepaper.matic.network> for more detail on the architecture and fraud proofs.

Github link to our contracts: <https://github.com/maticnetwork/contracts>

User and market adoption

We want to enable multiple systems for users to increase adoption like:

0x and other protocols

The Medium blog explaining how 0x will work on Matic:

<https://medium.com/matic-network/dex-on-matic-network-with-0x-7c1890590dab>

Note that 0x contracts can be deployed on Matic and that's why any relayer like Paradex will work on Matic. That way any user can trade instantly (~1 second) without waiting for block confirmations.

Payments

Matic will provide an interface for users and payment APIs and SDKs for DApps, merchant, and users to instantly accept or pay in crypto assets (e.g., ERC20 tokens, Ethers).

We have plans to roll out this system in three phases:

- Ethereum and ERC20 token payments
- Multi-asset cross chain transfer and payment through atomic swaps and liquidity providers
- Fiat enabled payment system through fiat liquidity providers

Lending platform

The Matic Network will enable a platform for merchants to assess the creditworthiness of connected users via their transaction history. This enables merchants to lend tokens to users on the network when transacting with users that do not have sufficient funds. This will use the Dharma protocol to provide tokenized debt to users.

Games

We expect games to be a big part of the Matic Network. In-game assets represented as NFTs (ERC721) are expected to be bought, sold and traded in huge numbers on our sidechains. Developers will also be able to save game state on the sidechains if they choose to. Along with the NFT marketplace that we will enable, developers and users will truly have a fast, efficient and secure sidechain to build and play games on.

Dagger

We have already started building infrastructure for developers, starting with Dagger; A notification engine to track Ethereum accounts and events in real-time.

You can learn more about Dagger here:

<https://medium.com/matic-network/ethereum-in-realtime-dagger-98ee2d717c76>

and check how it works: <https://medium.com/matic-network/understanding-dagger-453d90480c51>

Developers can use Dagger to track their own smart contracts, accounts, and transactions. They can create custom service or integrate with third-party services through IFTTT or Zapier.

We also launched our Ethereum app on Zapier. Using that, anyone can integrate Ethereum with thousands of other apps

Ethereum/Zapier invitation link:

<https://zapier.com/platform/public-invite/5455/044647aa32e38a80f68445871bcd6045/>

Matic Wallet

The Matic development team is working on building an easy-to-use Plasma wallet mobile app, integrated with WalletConnect, to ensure secure storage of keys, intuitive access to the features provided by the Matic Network, as well as a seamless mechanism to connect browser-based DApps to the mobile app. Users can interact with DApps on browsers and in the future many more devices, while still keeping their keys secure in their mobile wallet.

The Matic wallet will act as a ready tool for DApp developers to get their users onboard and working with Matic sidechains quickly and efficiently.

Research

Generalized State scaling

Generalized State scaling is the next frontier for the Matic Network, once the Matic Development Team is done with implementing micropayments, asset transfers and swaps in the first phase of development of the Matic Network. This is a research problem, and it will take time and effort to accomplish a breakthrough here.

There are mainly 3 different approaches that the team has been researching and working on:

- Stateful object programming model (separating code and state)
- State transition verification through zk-snarks
- State transition verification using an EVM-in-an-EVM construction