WHY WE'VE CHOSEN A PLASMA
like sidechain solution for our DEX

To innovate, you have to experiment. You need to try different things until you hit upon the one idea that beats the rest. We spent months exploring whether state channels or atomic swaps were the right basis for our decentralized exchange (DEX). We learned a lot from the experience, but to deliver the DEX of the future, we need a better solution.

The problem with state channels

State channels are off-chain networks that run parallel to the blockchain.

State channels made it possible to transact between multiple parties off-chain (as many times as you like) and only commit that block once the channel was closed, saving time and gas costs.

Since you avoid mining every single transaction, we believed this solved the scalability problem. But as the network grows and more transactions take place, you end up with an increasingly complex transaction history that each peer has to verify in order to trade. This puts incredible pressure on computing power for each peer in the network.

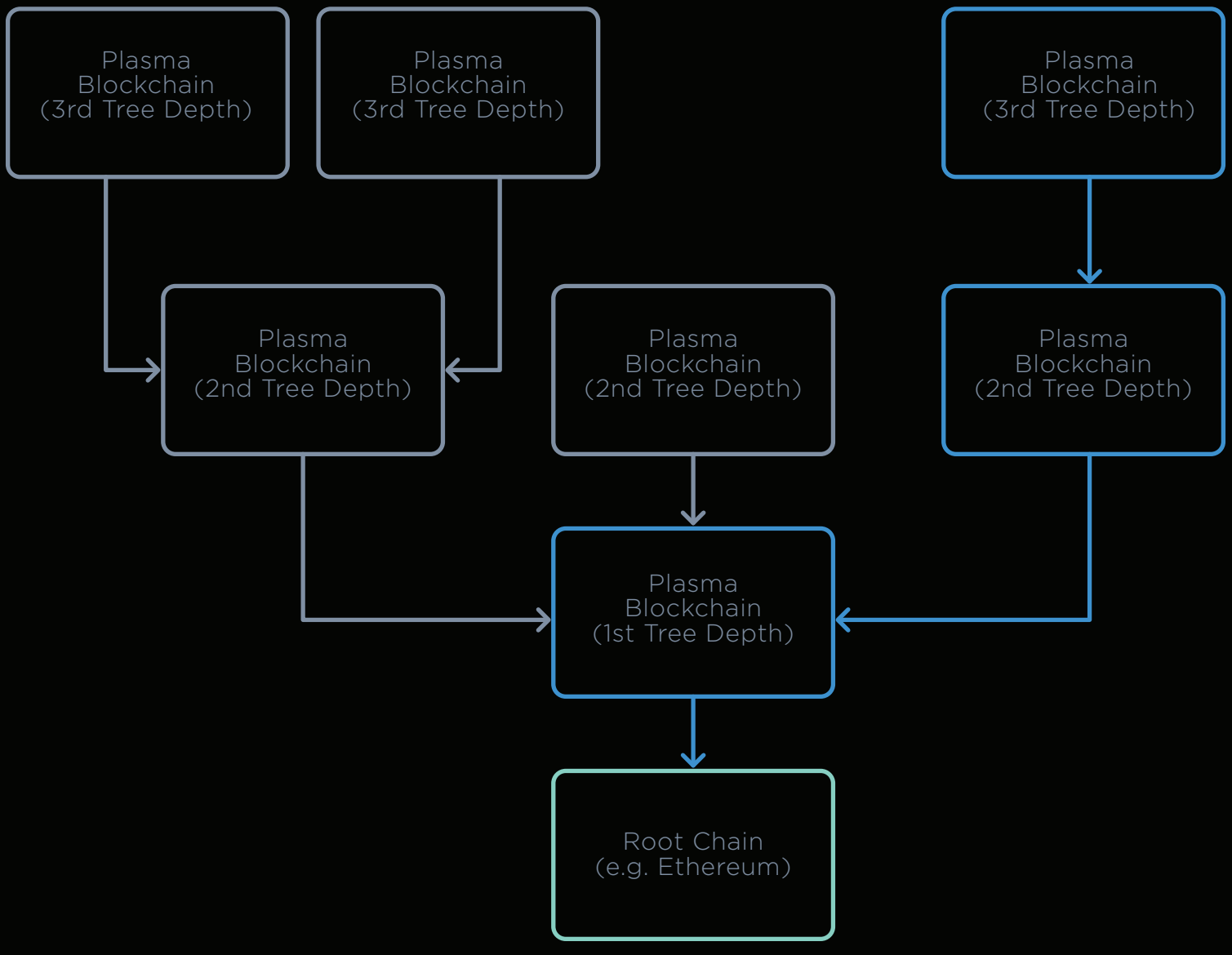
Before anyone can trade, they have to verify their trading partner's transaction history by verifying each of their trading partners and their histories, and so on. Depending on network activity, your computer would need to perform thousands or even millions of transactions before processing your trade. Few people have that kind of computing power. It slows transactions and increase fees, too. And that's not the kind of trading experience we want our users to enjoy.

Introducing Plasma:
WHAT IS IT?

Plasma was introduced by Vitalik Buterin (Ethereum) and Joseph Poon (Lightning Network) in their white paper, Plasma: Scalable Autonomous Smart Contracts.

In its most simplified form, Plasma is a design philosophy for off-chain applications. Plasma's goal is to scale Ethereum to transact billions of actions per second (instead of just 10–15) by building a blockchain within a blockchain, and removing the need for every node on the network to verify all transactions as they occur.

By splitting a blockchain by transaction type (DEX, dApp, social network, and so on), you can increase the transactional capacity in proportion with the number of divisions. For example, you could create a sub-chain on Ethereum for a DEX, operating independently on a Proof-of-Stake consensus mechanism, that effectively doubles transactional capacity. Three chains would triple it, four quadruples it, and so on, ad infinitum (in theory).



The state of each sub-chain is enforced by its “parent” or “root” chain, but it doesn’t need to do anything unless there’s proof of fraud, which is another reason why Plasma can support so many transactions.To withdraw funds, traders wait a predetermined period of time to ensure other nodes can challenge any fraudulent activity. In the case of proven fraudulent behaviour, Plasma will trigger a “mass-exit”, which allows users to withdraw their funds from smart contracts (after proving ownership from the last legitimate block in the chain) while the fraudulent block is reversed.

There’s theoretically no limit to the number of sub-chains, so Plasma solves the scalability problem while still providing a secure, decentralized trading environment.

The Altcoin.io sidechain

In order to create a DEX that ensures instant, trustless trading, we’re going to use a similar idea to Plasma.

We’ve partnered with Tendermint, a consensus technology that’ll operate a Proof-of-Stake (PoS) mechanism for nodes in our DEX. Each node will sign transactions and commit them to blocks. Currently, Tendermint can handle up to 10,000 transactions per second, and as we only commit transactions for our DEX, we’ve massively improved transactional capacity without sacrificing security.

When trading through Altcoin.io, you’re effectively trading on a sidechain that reports to a smart contract on Ethereum. The smart contract is there to ensure everyone in the sidechain, including us, plays by the rules. Trading will be trustless, near instant, and our DEX will have an in-built mass-exit function to ensure that if verifiers spot fraudulent activity, you won’t lose your funds.

When can you try it?

We plan to release the first version of our Plasma-like DEX soon that combines the advantages above with an incredible user experience. Whether you’re a novice just getting into cryptos or a seasoned pro looking for a better trading platform, we’ve designed every aspect of Altcoin.io to be intuitive, fast, and safe.