CrushCrypto

Layer 2 Blockchain Scaling Solutions – Sidechains

Educational Series

November 9, 2018

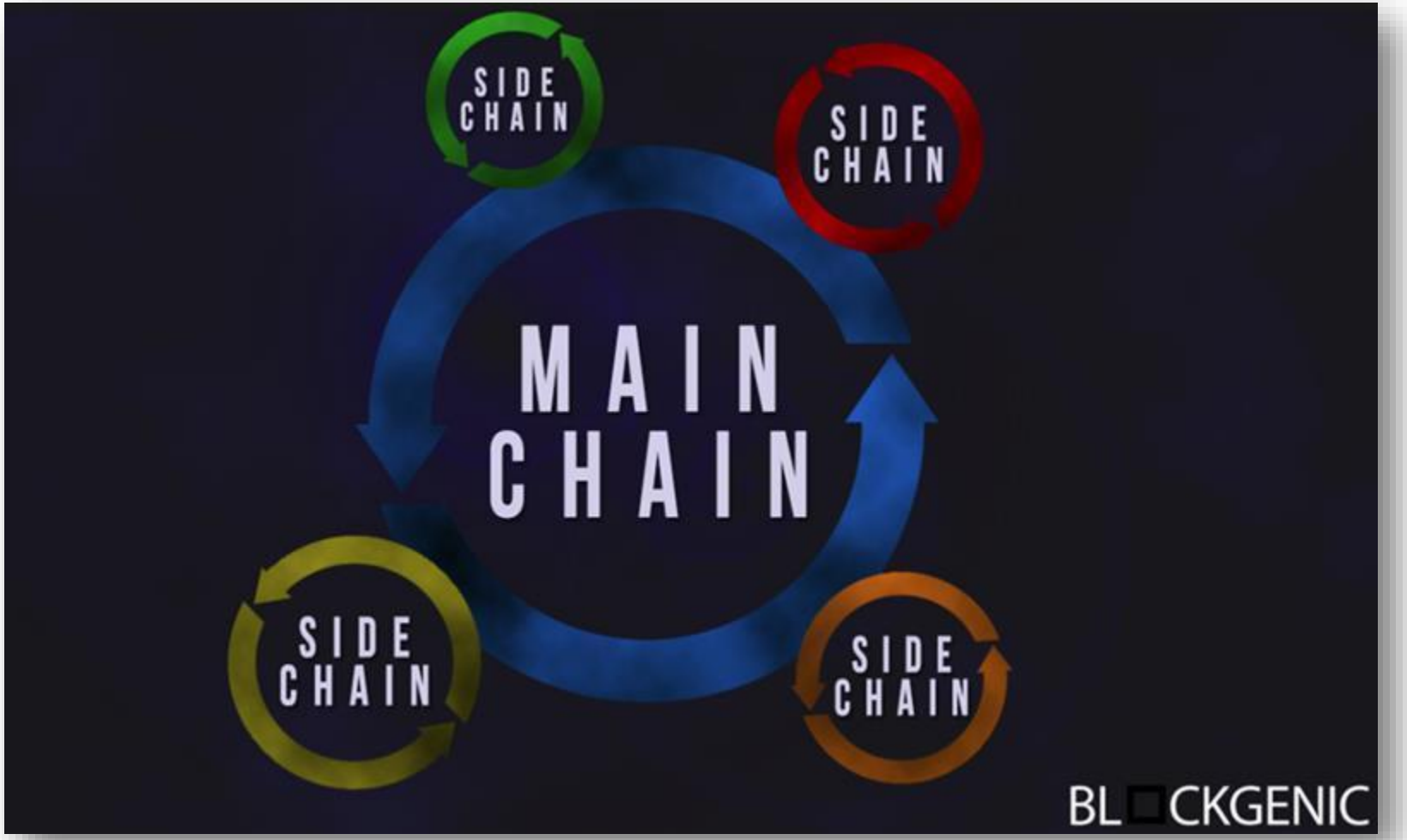
What are sidechains?

- A **sidechain** is a unique blockchain that is attached to a **main-chain** using a two-way peg. Sidechains allow tokens and digital assets from one blockchain to be used in a separate blockchain and then moved back to the original chain if needed.
- Sidechains are independent form the main-chain and are responsible for their own security, meaning they need a mechanism for achieving consensus while protecting from bad actors. Their independence also means that if a sidechain is compromised, it will have no impact on the operation of the main-chain.
- Sidechains are a promising **layer 2 scaling solution** because it allows for transactions to be conducted off the main-chain, similar to state channels. People can send funds and use dApps through a sidechain, which takes pressure off the main-chain and allows for it to operate with faster and cheaper transactions.

Issues with sidechains

- Sidechains are not perfect and there are still issues to be solved if they are going to be implemented as a widespread solution for scaling. Due to their independence from the main-chain, there are security concerns about mining power and easier 51% or Sybil attacks.
- Another issue is that sidechains add another level of complexity to blockchain technology for new users. There are also unanswered questions about what exactly would happen to assets in the event of a sidechain being compromised or failing. A lot of research is being done on providing security to sidechains using different methods.

Sidechain visualization



How do sidechains work?

- Sidechains are independent blockchains responsible for their own security and simply connected to a main-chain through a two-way peg.
- Each sidechain needs to have miners (if using a proof-of-work consensus mechanism) or block producers/validators if using a different consensus mechanism. They can interact with the main-chain, but what happens to the sidechain does not directly impact the main-chain and vice versa.
- To trade assets from the main-chain to the sidechain, a user needs to send their assets on the main-chain to a specific address that locks up the funds. After the transaction is confirmed, a notification is sent to the sidechain and a certain amount of sidechain assets are credited to the user (the exact amount depends on a set exchange rate).
- To trade assets from the sidechain to the main-chain, the process would be the same except reversed.

Federations

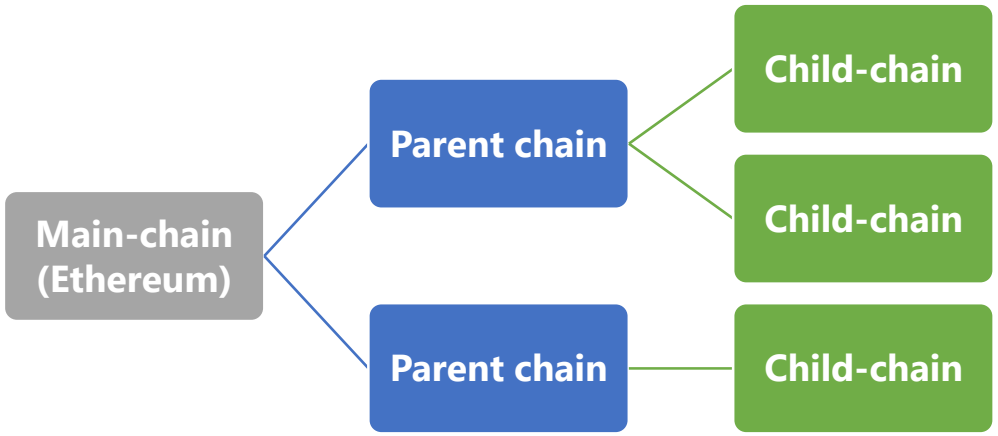
- Certain sidechain implementations utilize some kind of federation.
- A **federation** is a group of servers that act as an in-between point between the main-chain and sidechain.
- Federations decide when the user's coins are locked as well as released, and sidechain developers can choose members of the federation.
- Note that most federation design is not trustless - hence, there is a risk of centralization depending on how the federation is designed and selected.

Plasma overview

- One prominent implementation of sidechain technology is **Plasma**. In August 2017 Joseph Poon and Vitalik Buterin released the first draft of the Plasma whitepaper.
- In the paper, they describe an Ethereum scaling solution “which is scalable to a significant amount of state updates per second (potentially billions) enabling the blockchain to be able to represent a significant amount of decentralized financial applications worldwide.” utilizes the security of the Ethereum blockchain while providing users with sidechain benefits like transaction speed and cost.

Plasma overview (continued)

- Plasma is a framework for the creation of sidechains (called **child-chains**) that interact with the Ethereum blockchain. These child-chains can have their own child-chains, etc.
- The Plasma framework can be thought of as a hierarchical tree of sidechains that conduct transactions and computations on their own and periodically transfer information to the main-chain.
- The benefit to this structure is that developers can run entire applications on child-chains, operating at faster speeds and lower fees than the Ethereum blockchain itself.

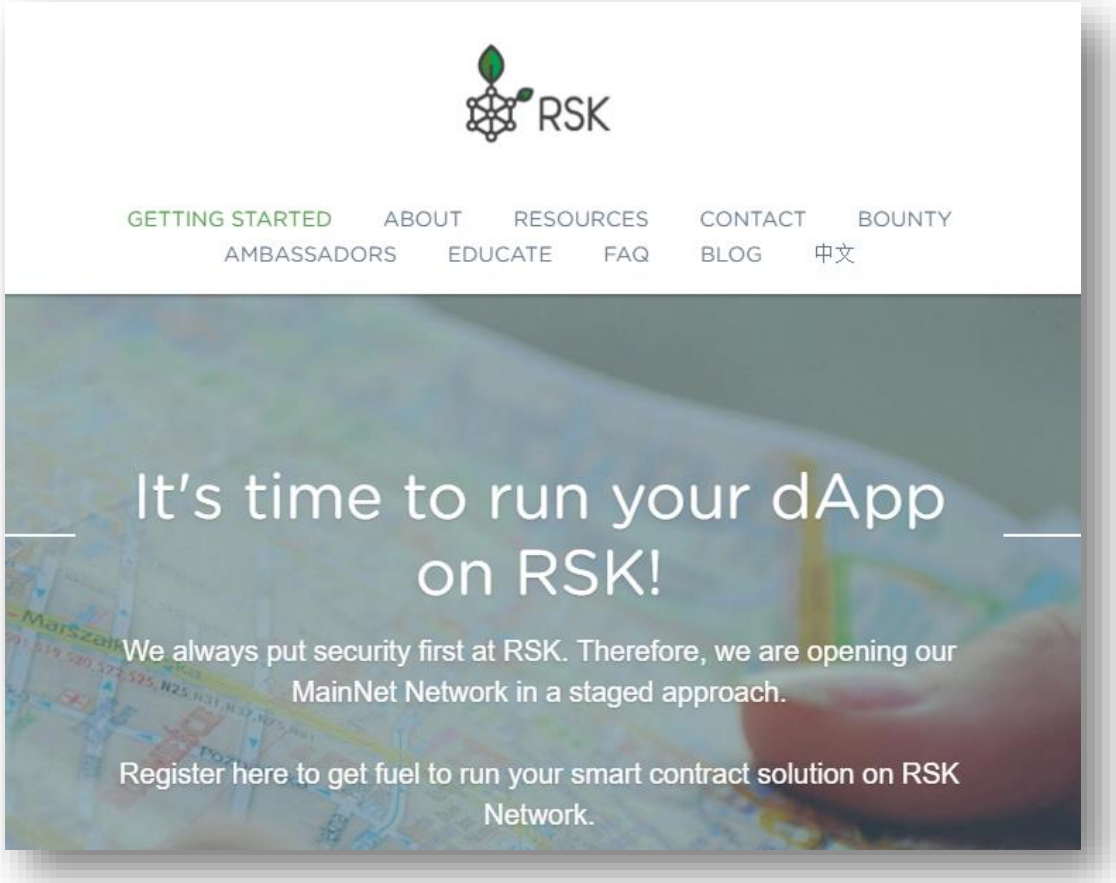


Plasma overview (continued)

- To create a Plasma child-chain, a smart contract is created and deployed to the Ethereum main-chain. This smart contract contains the rules and state hashes of the child-chain and contains the two-way peg that allows users to transfer assets between the main-chain and child-chain.
- When a child-chain is up and running, the block creators must periodically send information to the main-chain with the purpose of proving the validity of the child-chain according to its consensus rules. This is how the Plasma framework utilizes the security of the Ethereum blockchain while providing users with sidechain benefits like transaction speed and cost.

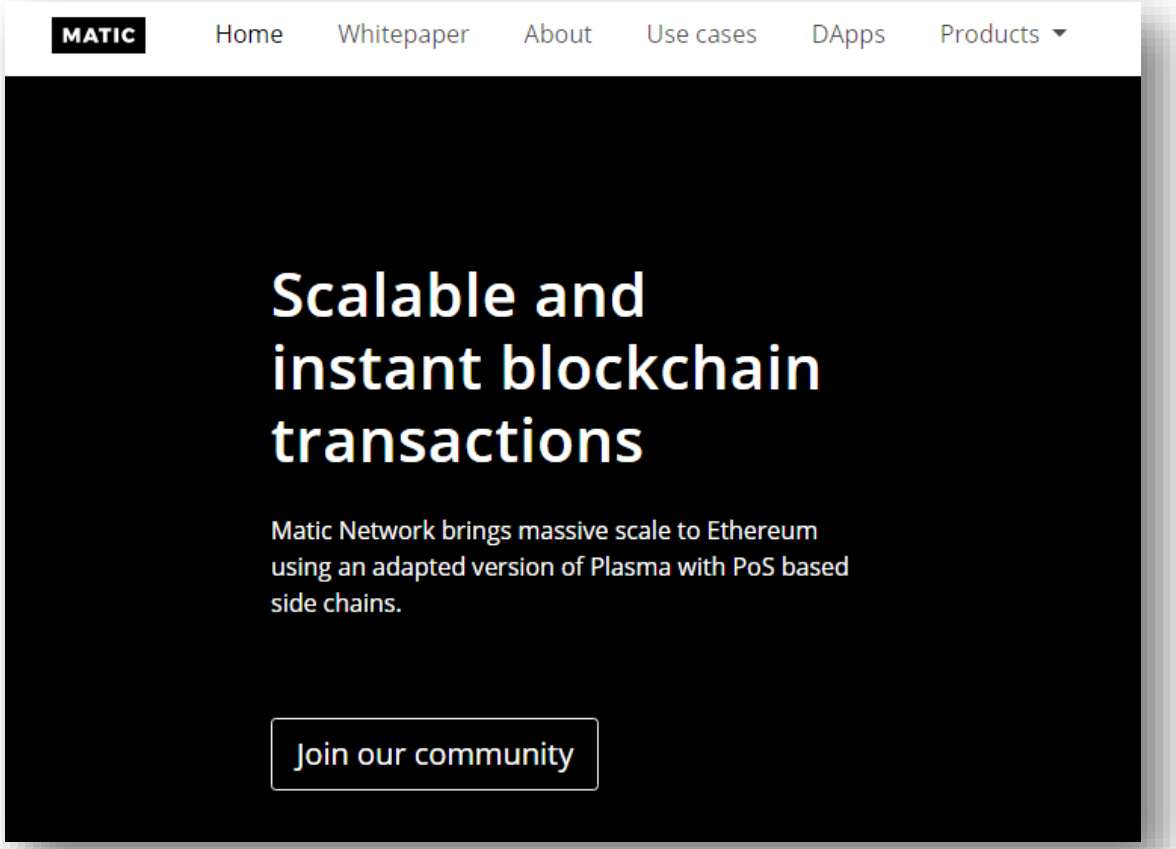
Projects working on sidechains: RSK

- Website: https://www.rsk.co
- An open-source smart contract platform with a two-way peg to the Bitcoin blockchain that also rewards Bitcoin miners via merge-mining, allowing them to actively participate in smart contract resolution.
- The goal of RSK is to add functionality to the Bitcoin ecosystem by enabling smart contracts, near instant payments, and higher scalability.



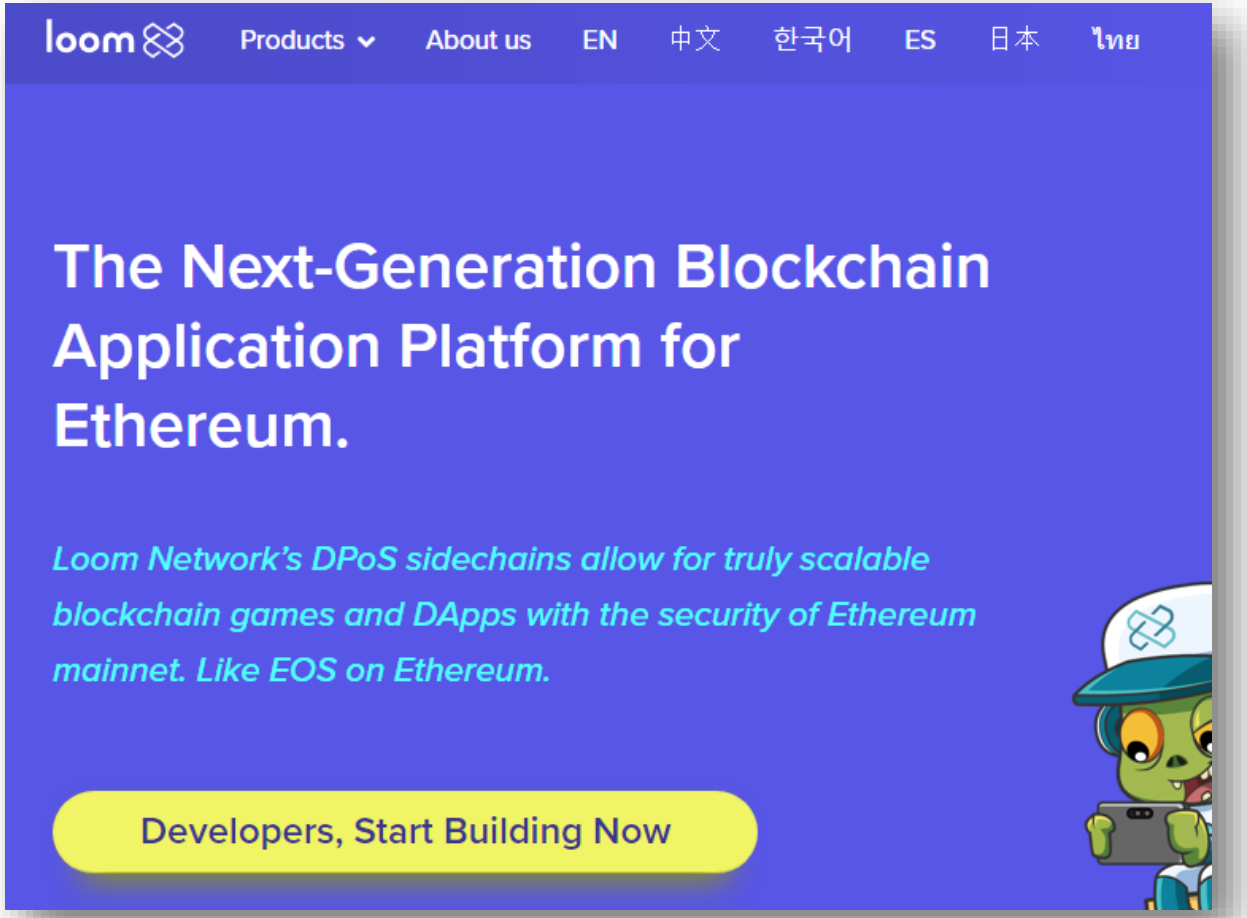
Projects working on sidechains: Matic Network

- Website: https://matic.network
- A decentralized platform that uses an adapted version of the Plasma framework discussed in the above section. Some of the features include account-based Plasma, decentralized validator layer, and the focus on user experience.



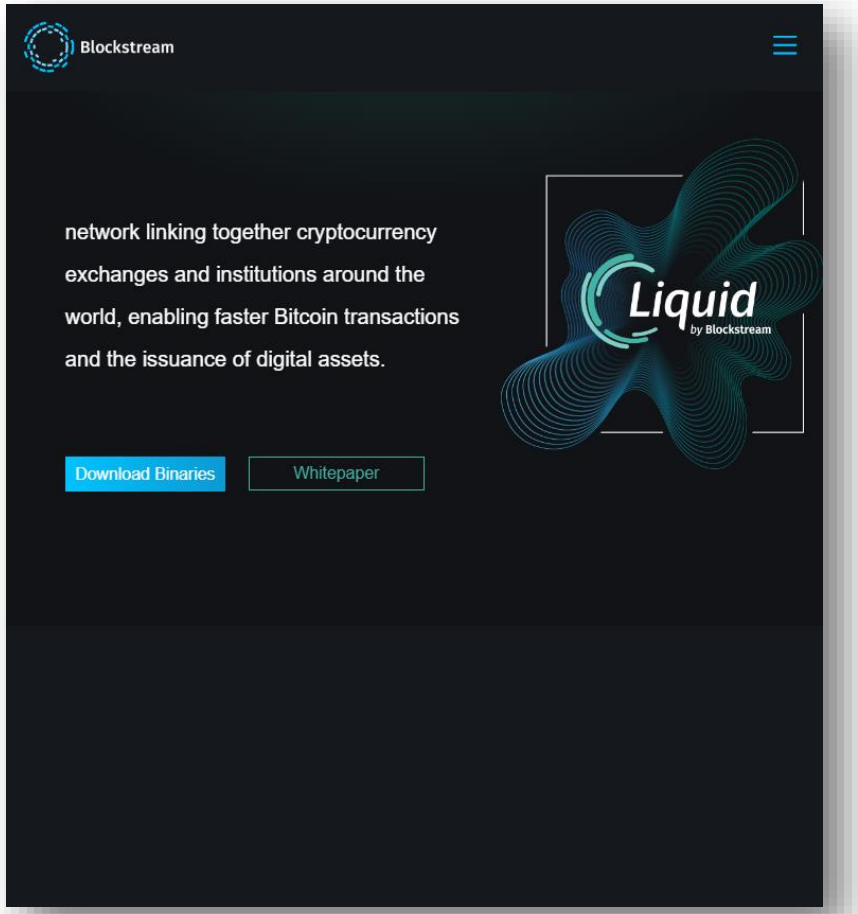
Projects working on sidechains: Loom Network

- Website: https://loomx.io
- A network of sidechains connected to Ethereum that use a delegated proof-of-stake consensus mechanism. These sidechains allow developers to build highly-scalable games and user-facing dApps that are backed by the security of the Ethereum blockchain.



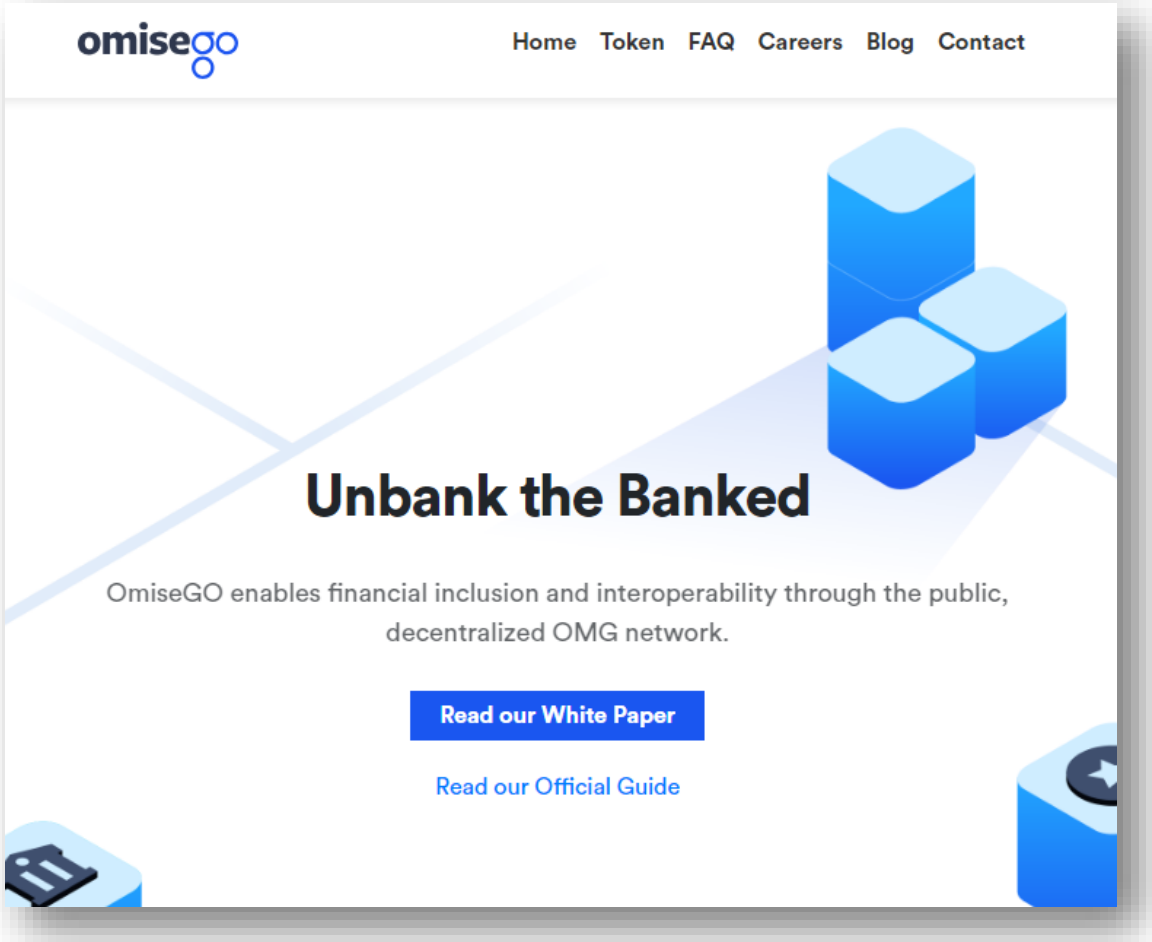
Projects working on sidechains: Liquid

- Website: https://blockstream.com/liquid
- A production sidechain and inter-exchange settlement network for Bitcoin utilizing a federation as nodes that was created by Blockstream.
- The goal is to improve capital efficiency and market liquidity by facilitating rapid and secure transfers between accounts at participating exchanges or brokerages.
- After 102 confirmations (approximately 17 hours) on the Bitcoin blockchain, the synthetic Bitcoin LBTC on the side chain is transferred to the user.



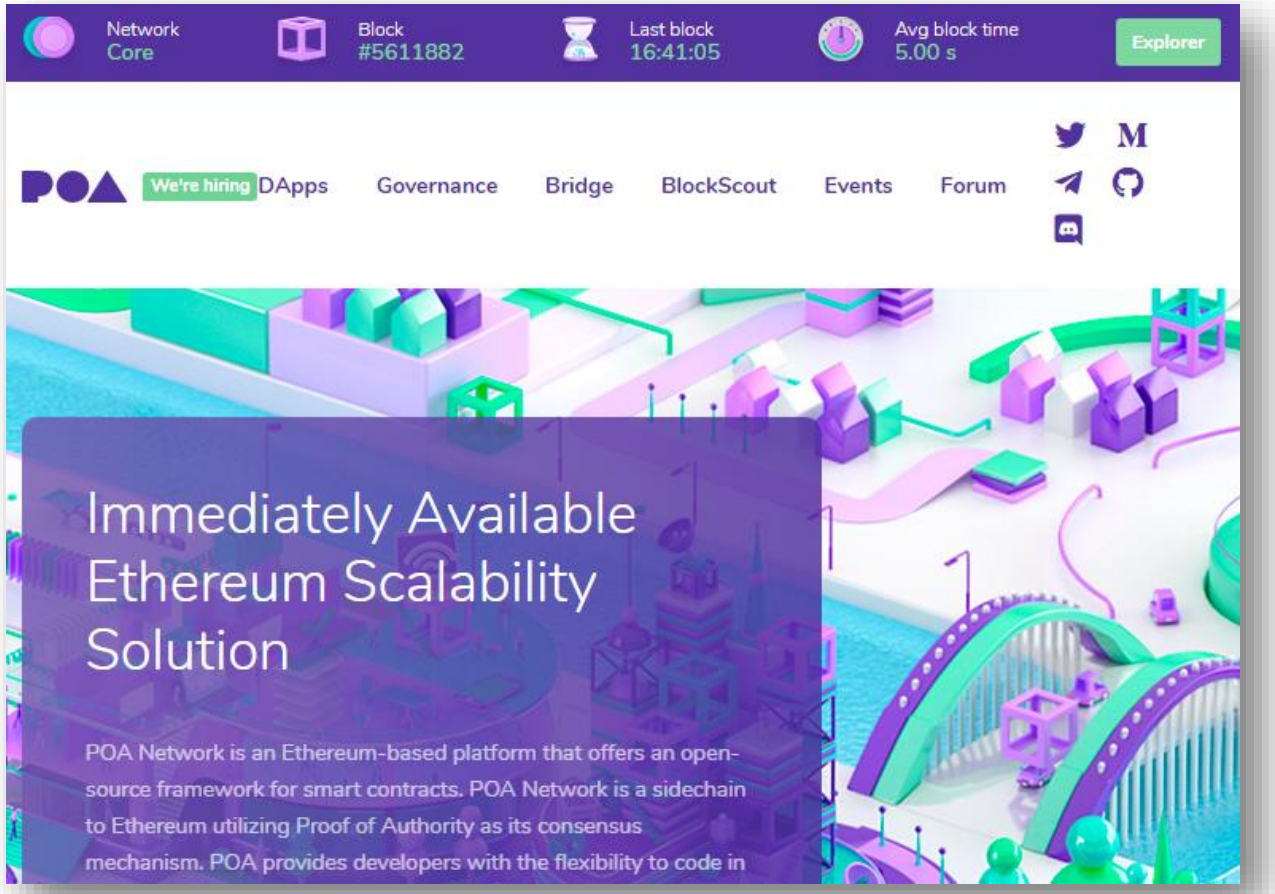
Projects working on sidechains: OmiseGO

- Website: https://omisego.network
- A public, currency agnostic decentralized exchange network that will be secured by Ethereum and built to scale using Plasma architecture.
- The network will be able to interact with Bitcoin and other blockchains and is being built with a high capacity for scalability.



Projects working on sidechains: POA Network

- Website: https://poa.network
- An Ethereum-based platform offering an open-source framework aimed at providing easier, cheaper, and faster execution of smart contracts.
- It is a sidechain to Ethereum that uses proof of authority (PoA) as its consensus mechanism.



CrushCrypto