Plasm Network and Layer 2

Silesia Presentation - Plasm Network

0.Little bit about the team

The Team

CEO Sota Watanabe

Co-founder and CEO at Stake Technologies. A researcher at the University of Tokyo. (2019.4-2020.4) ex-Chronicled.

CTO Takumi Tamashima

Co-founder and CTO at Stake Technologies. Nominated one of the 16 best U25 engineers in 2018 by Japanese government.
Master at The University of Tokyo.

COO Masaharu Uno

COO at Stake Technologies.
ex-Omise country manager.
ex-Securitize Japan vice president.

PM Yoshinobu Shijyo

ex-executive and CTO at several Japanese blockchain companies.
PhD at Osaka University, and graduated Osaka University (Bachelor) at the top of graduation list.

Core Developer Task Ohmori

Silver medalist of the international physics olympics in 2012 and 2013.
Master at the University of Tokyo.

Core Developer Aleksandr Krupenkin

One of the first Ethereum and Polkadot contributors. ex-Robonomics.
Lead developer of Plasm Network.

Software Engineer Kim Hoon

Developer of Plasm Network.
His graduation paper using Substrate won the first prize at Asia Pacific University. (APU)

Engineer Tomomasa Matsunaga

PhD student at The University of Tokyo

Speaker - Hoon Kim

- Graduated from Ritsumeikan Asia Pacific University.
- International management major
- Graduation thesis on distributed stock exchange with Substrate
- Part of the Plasm dev team
- Developed the Lockdrop web app
- Loves to play and make games!

@hoonsubin

hoonkim@stake.co.jp

1.Introduction to layer 2

What is layer 2?

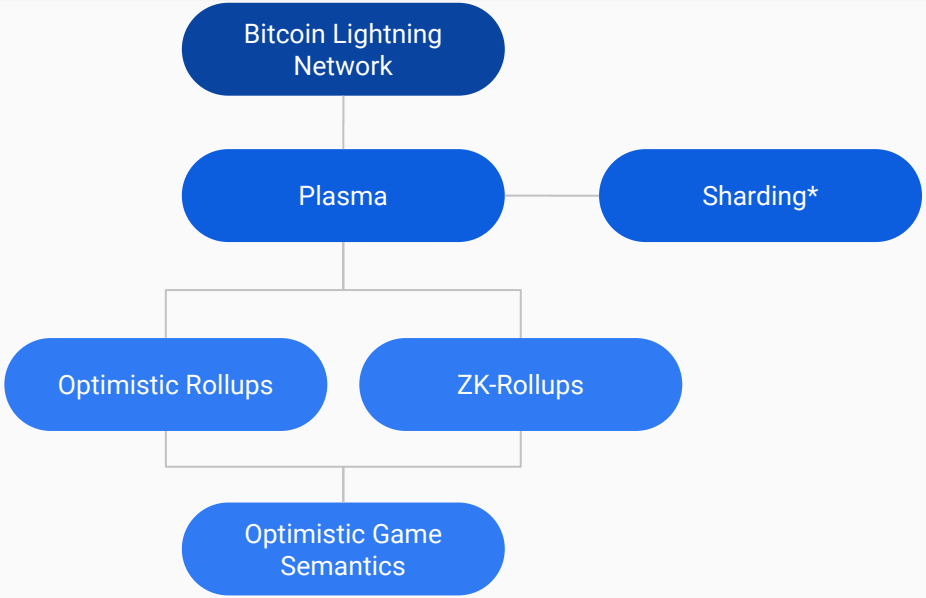
“Layer 2 refers to a secondary framework or protocol that is built on top of an existing blockchain system. The main goal of these protocols is to solve the transaction speed and scaling difficulties that are being faced by the major cryptocurrency networks.”

- Binance Academy

Basically...

Off-chain on sterolds

A brief history of L2

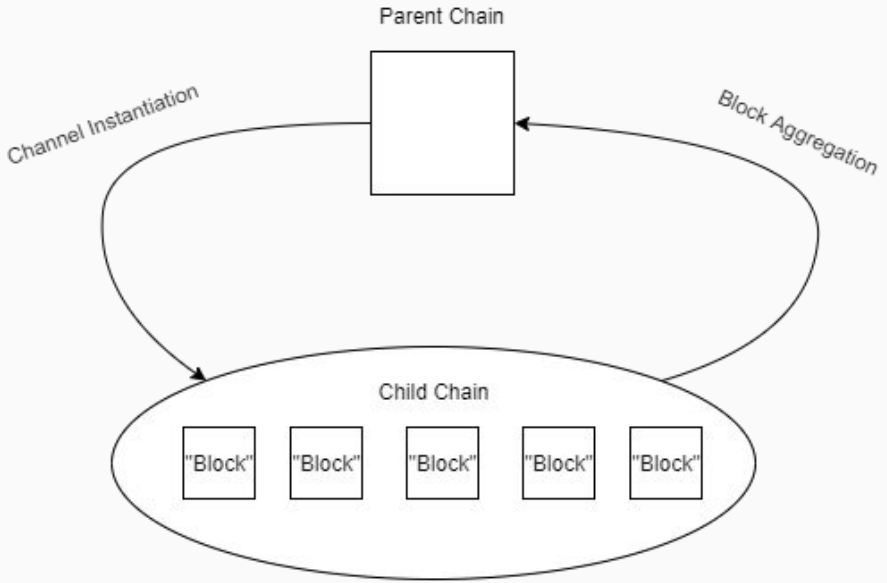


*)Sharding is not layer 2

Generic layer 2 at a glance

In short, layer 2 is all about moving the transaction off-chain and process them in chunks. Starting from simple payment channels, to handling smart contract transactions with its own block validation.

Layer 1 (root or parent chain) contains the *facts*, while layer 2 (child chains) handles the transaction and sends them to the parent chain for confirmation and consolidation.



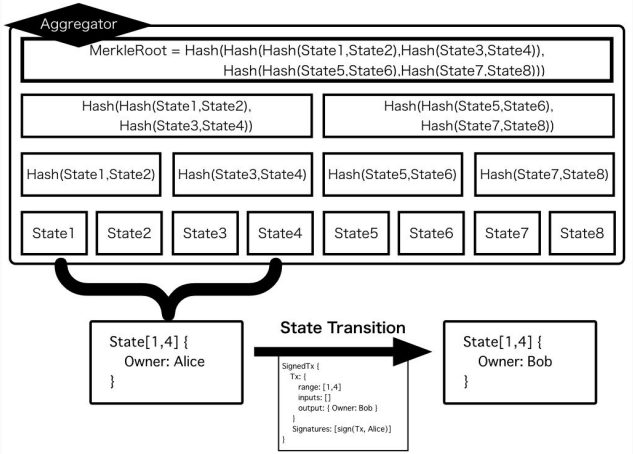
Transaction fee only occurs when:

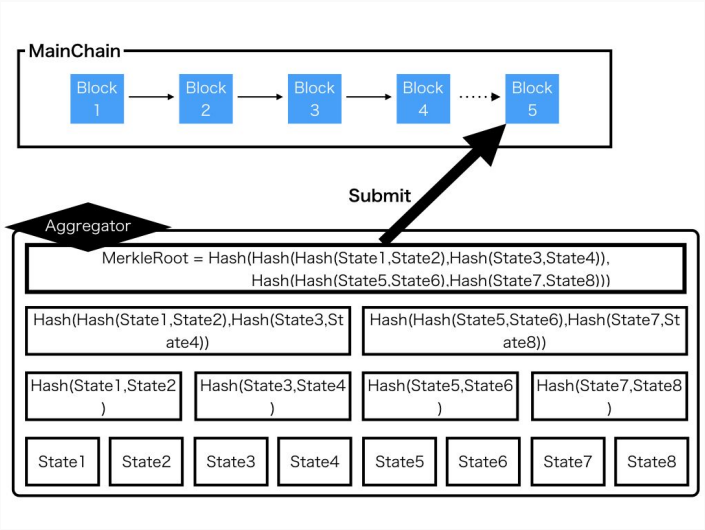
1. Instantiating a channel
2. Moving the state transitions back to the root

Smart Contracts and *Merkle trees* are used to bridge the parent chain to the child chain

dApps on layer 2

Child chains are essentially a small blockchain with its own EVM (works via a Merkle Tree) that pulls and pushes information from the main chain





How secure is it?

There are several built-in security features like:

- Fraud-proof
- Community votes
- Staking/Bonding
- Reverting back to root

The root chain is the judge

Other nodes can claim that a child chain is fraudulent (ex: hash x does not exist).

The child chain must go through a Verification Game to prove that the hash exists. Or else, the state is reverted back to the root chain.

This is done by the root chain validator nodes and the contract that handles this is called a Predicate contract.

When a logical error occurs on a child chain, the aggregators bond in the child chain contract will be slashed and be allocated to the validator.

2.Different Protocols

State Channels

Probably the simplest and oldest layer 2 protocol.

Uses a instant payment channel to handle transactions off-chain.

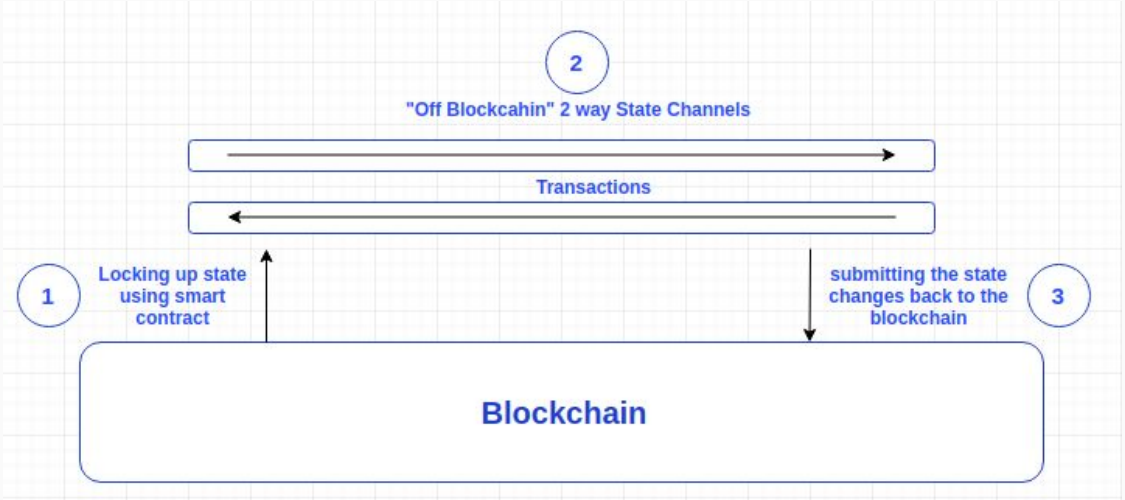


Image by ETH Hub

Payment Channels

An application of State Channels.

It uses a Raiden Network which allows secure transfers of tokens between participants without the need for global consensus. This is achieved using digitally signed and hash-locked transfers, called balance proofs, fully collateralized by previously setup on-chain deposits.

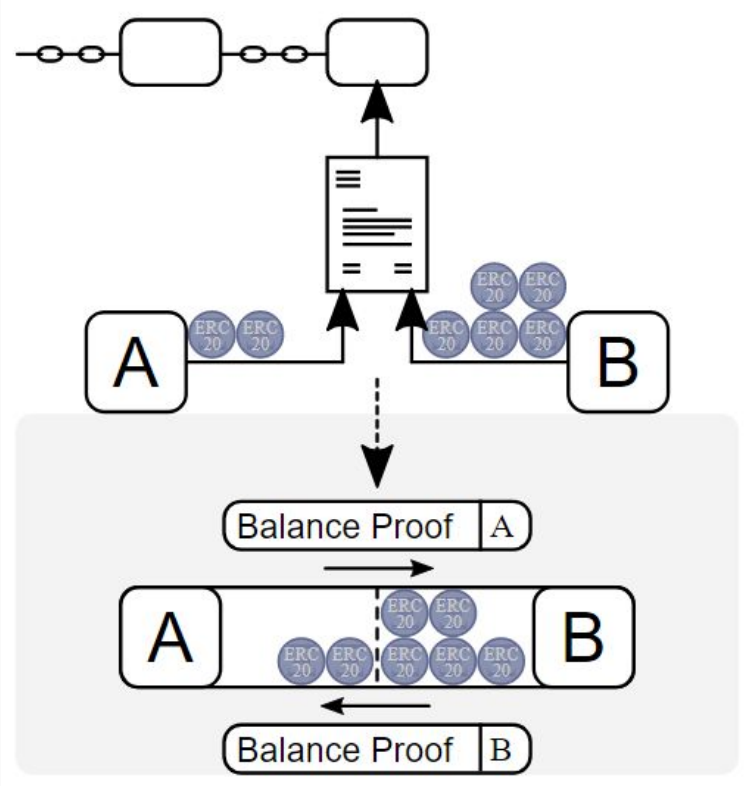


Image by ETH Hub

Plasma

The Plasma structure is built through the use of smart contracts and Merkle trees, enabling the creation of an unlimited number of child chains - which are, essentially, smaller copies of the parent blockchain. Each chain is designed to work in a singular way, serving different needs by coexisting and operating independently. On top of each child chain, more chains can be created and this is what builds a tree-like structure.

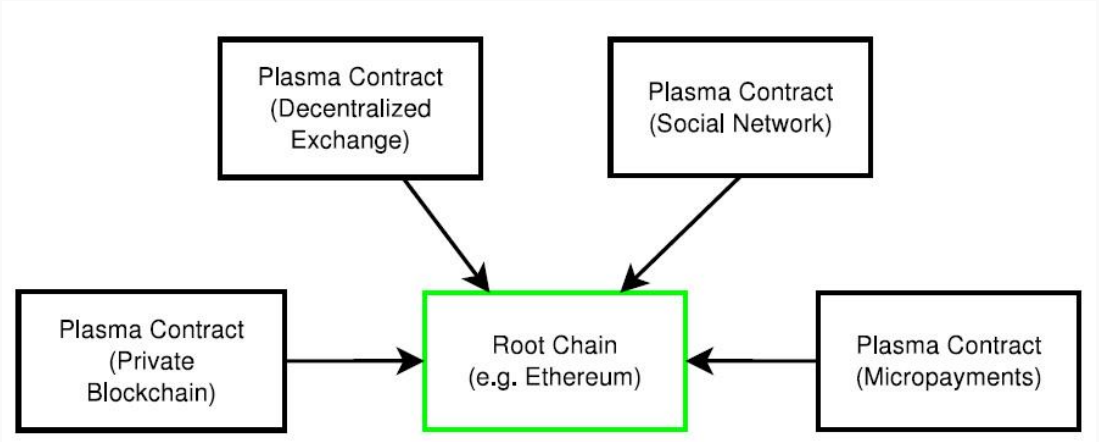


Image by Joseph Poon & Vitalik Buterin

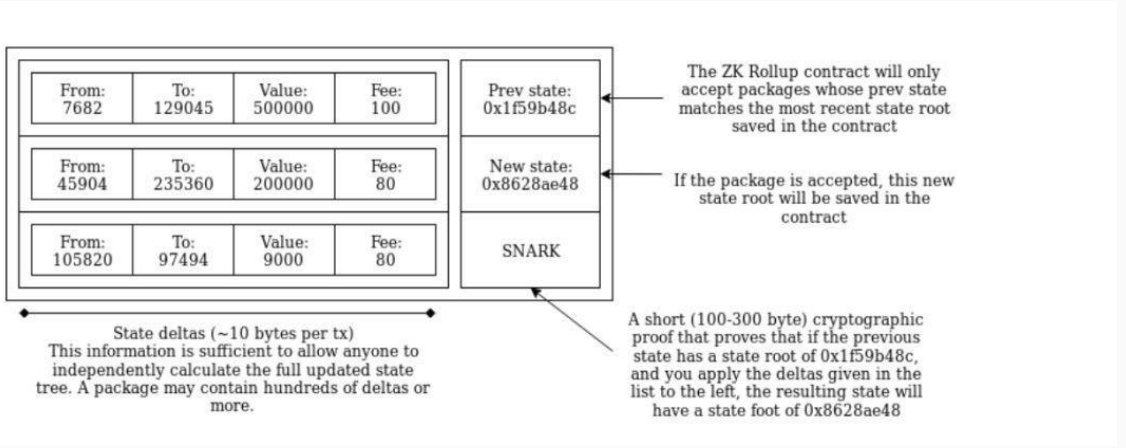
Optimistic Rollups

Optimistic Rollups (ORs) enables running smart contracts at scale while still being secured by the parent chain. These constructions resemble Plasma, but trade the almost infinite scalability of Plasma to run an EVM compatible Virtual Machine.

1. A user sends a deploy transaction of a smart contract off-chain to an aggregator (a block producer in this construction)
2. An aggregator locally deploys the transaction creating the new smart contract
3. That aggregator computes the new state root (aka a merkle root)
4. The aggregator creates a transaction which contains that state root calculated in step 3 to the root chain

ZK-Rollups

ZK-Rollups bundle hundreds of transfers into a single transaction. The smart contract will deconstruct and verify all of the transfers held in a single transaction. A "zero knowledge proof" approach is used to present and publicly record the validity of the block on the parent chain. ZK reduces computing and storage resources for validating the block by reducing the amount of data held in a transaction; zero knowledge of the entire data is needed.



Transactors create their transfer and broadcast the transfer to the network. The transfer data consists of an indexed "to" and "from" address, a value to transact, the network fee, and nonce. The smart contract records the data in two Merkle Trees; addresses in one Merkle Tree and transfer amounts in another.

Relayers collect a large amount of transfers to create a rollup. It is the relayers job to generate the SNARK proof. The SNARK proof is a hash that represents the delta of the blockchain state.

3.Unifying layer 2

Optimistic decision

Layer 2 is aware of layer 1's state and tries to guess the next state to enable fast and safe transactions for both L1 and L2. This is done via a Predicate contract.

Narrowing down the possible future of L1 in the context of L2 is called the Optimistic Futures Cone.

1. Look at L1, and figure out what could possibly happen in the future.
2. Look at off-chain messages and what they guarantee if used in L1.
3. Restrict our expectation of future L1 state based on those guarantees.

OVM

A virtual machine that is developed to unify most, if not all of the layer 2 protocols into a single language that can communicate with the predicate module and the main chain's virtual machine (i.e. EVM or EWASM).

OVM is the bridge between L1 and L2. With OVM, you can convert a smart contract language (like Soldity) to leverage the predicate module and work with L2.

Demo: https://ovm-compiler.netlify.app/

4.Introducing Plasm Network

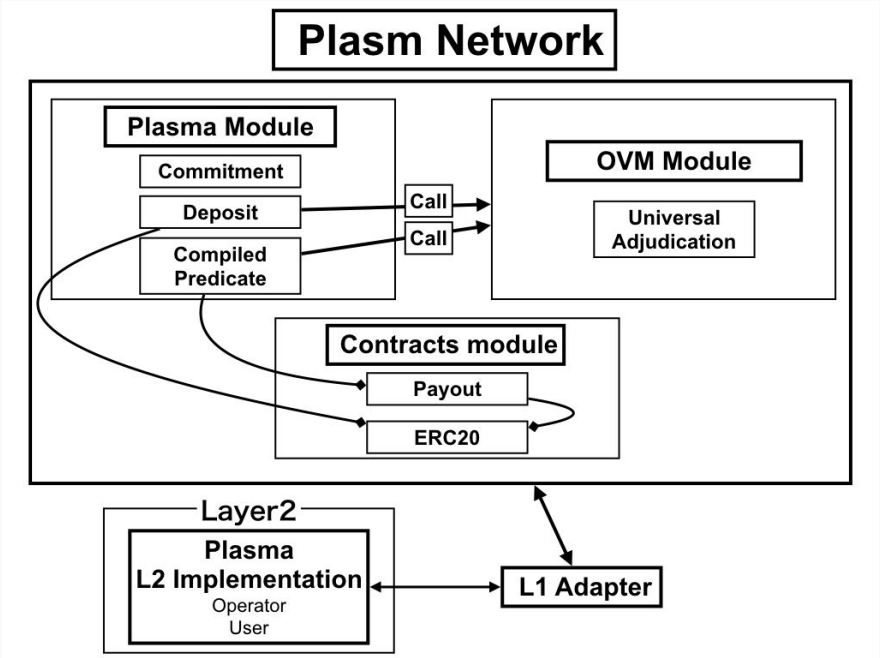
Main Features of Plasm Net

1. OVM module
2. dApp operator rewards
3. Operator trading
4. Multi-lockdrop

OVM Module

OVM is part of the runtime pallet for Plasm Network. Plasm is developed with L2 solutions in mind. We implement OVM for ink! Contracts on Substrate.

Smart contracts on the Network can leverage L2 protocols without the overhead that traditional implementation (such as setting up a predicate contract) has



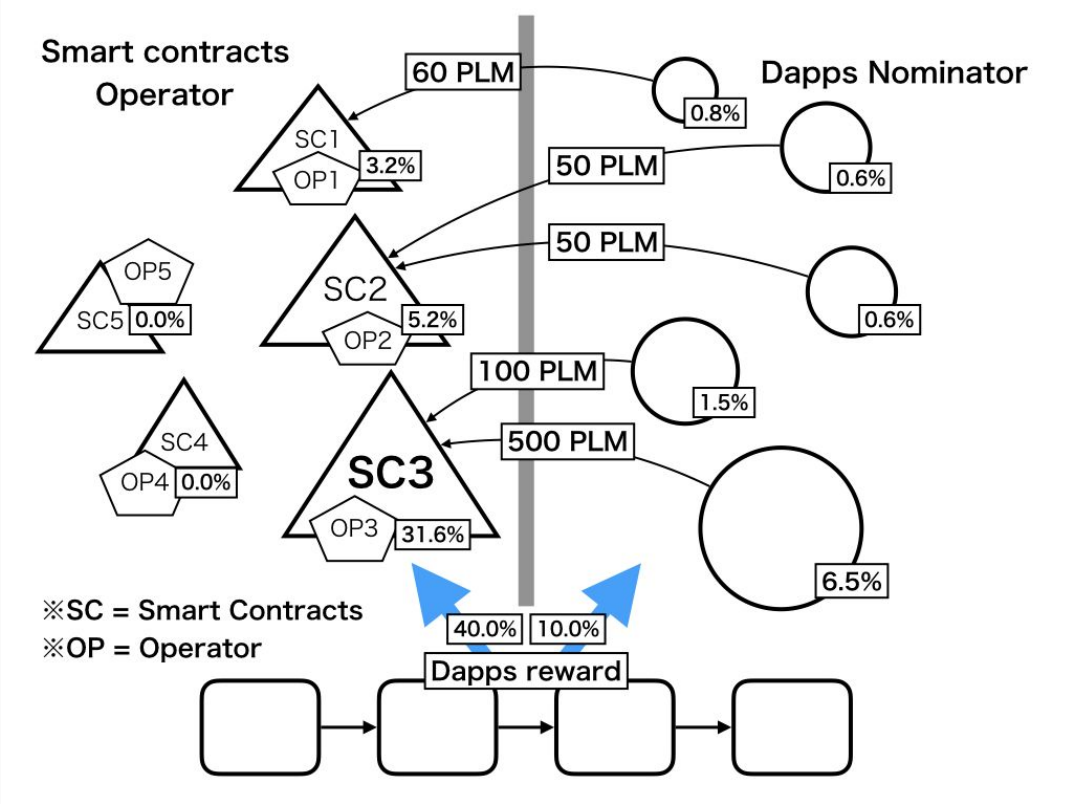
dApp operator rewards

Splits the block validation reward by half and allocate it to Nominated contracts and the Nominator

Nominating a contract is like investing in a dApp project, but with systematic rewards

The amount of receiving reward is proportional to the number of stakes in the contract

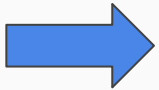
Rewards are issued each Era, acting as a basic income for the developers



dApp operator rewards cont.

Risks:

- Someone stakes to their own contract (freeriding)
- The network having disproportional nominations



Mitigations:

- Using community votes to slash malicious freeriding dApps
- Option to receive reward at a higher rate for dApps with few nominations

Operator trading

In this context, “Operator” refers to the owner of a smart contract (i.e. the address that can receive the dApps rewards)

In Plasm Network, you can switch the address of a smart contract Operator

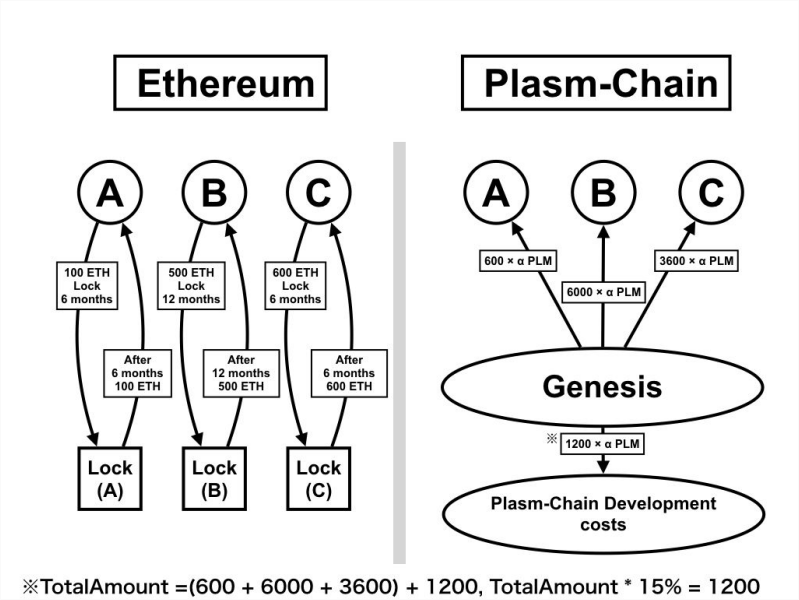
This system is implemented in hopes of making dApps as a viable business in the off-chain world

Multi-lockdrop

Lockdrop is a new token distribution mechanism

Instead of having just distributing (minting) the tokens once, Plasm Network will repeat this three times

Our third lockdrop, the DOT lockdrop will have some special treatments that we'll discuss later



Locked days	LockBonus
30-th	×24
100-th	×100
300-th	×360
1000-th	×1600
About 2-years (※DOT only lockdrop)	×2000

16,783.2 ETH

368 locks were made in a span of 1 month!

5.Substrate, Polkadot and Parachains

The Blockchain Framework - Substrate

- A blockchain framework developed in Rust.
- Made with modularity in mind
- Easy to jump start any blockchain projects
- Blockchains made with Substrate can become a parachain by implementing the Cumulus module
- Smart contracts are written in ink!, a eDSL in Rust that compiles to WASM

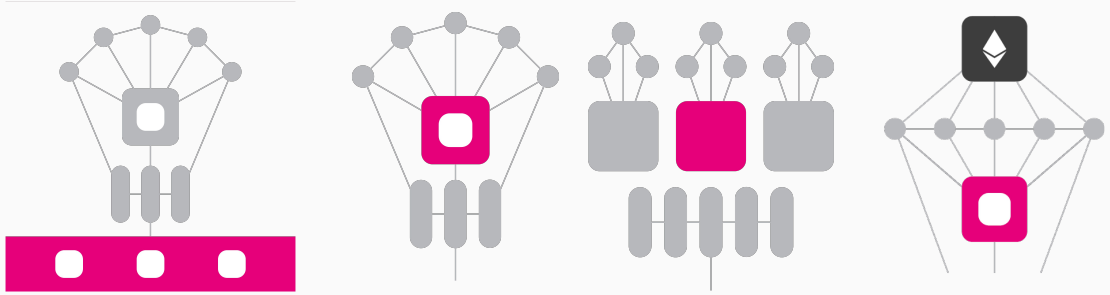
The Polkadot Network

A heterogeneous blockchain network that focuses on interoperability between different blockchains through various methods

Polkadot supports shared consensus and cross-chain messaging protocol (XCMP) for interchain transactions amongst its *shards*

Polkadot uses a NPoS consensus mechanism

Polkadot.



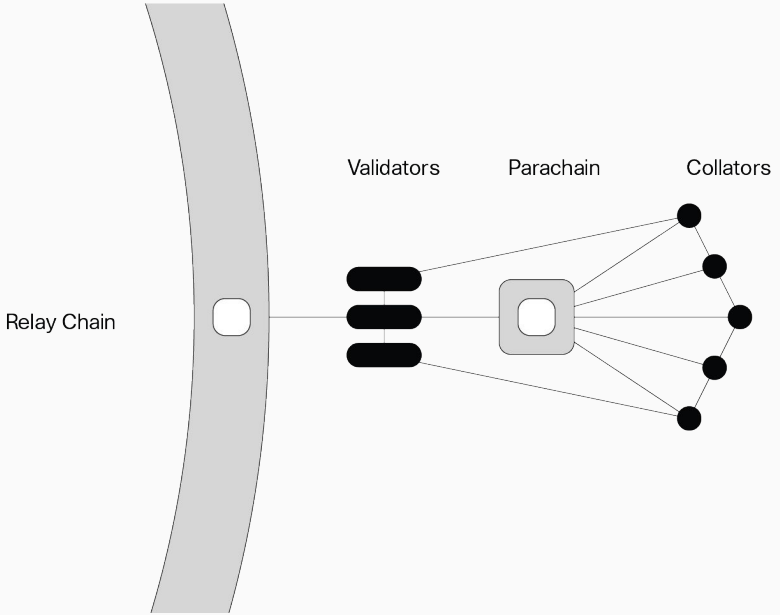
Relay Chain Parachains Parathreads Bridges

Parachains

Parachins are separate blockchains that works alongside Polkadot Network. They are also a shard of Polkadot

Parachains works on a shared consensus that the Relay Chain provides, allowing the developer to make a network that doesn't have to think hard about block validation!

But not everyone can become a parachain

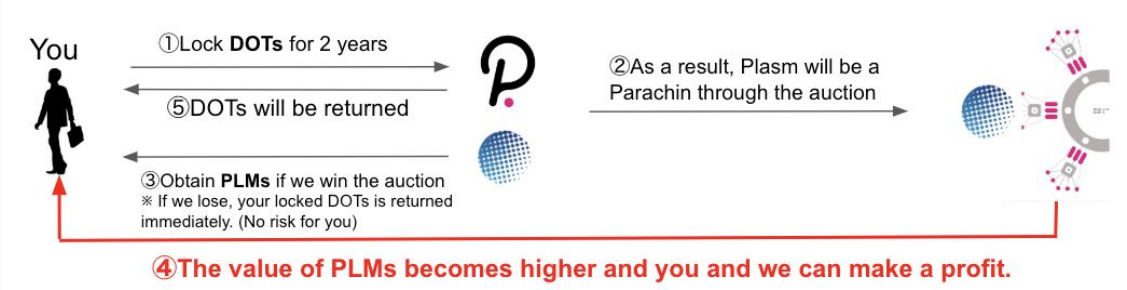


Parachains are maintained by collators. They are responsible for sending state transition proofs to the validators

Plasm Network Parachain Auction

There are only a limited number of parachain slots for Polkadot Network. These slots will be allocated via a candle auction

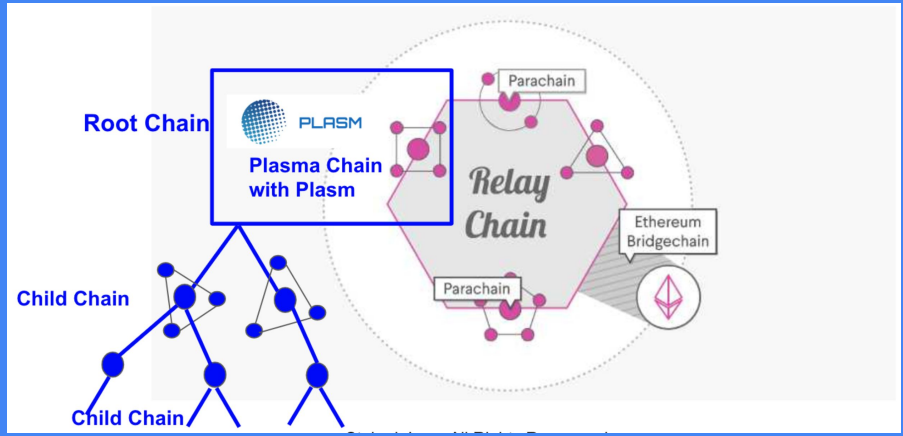
Bidding is done via DOTs and the blockchain with the most continuous bid (divided into 4 periods tallying up to 2 years) gets a slot



The 3rd lockdrop of Plasm Network will include the option to “lock” DOTs.
This option will only allow for 2 years lock, but has greater return in PLM (compared to that of other token locks)

The ultimate scalability

Plasm Network as a parachain is both horizontally and vertically scaling



Thank you!

Contact us:

Stake Technologies

hoonkim@stake.co.jp

https://www.plasmnet.io/
https://discord.gg/rRFcwJM

PLASM

project supported by
web3 foundation
grants program

Further Readings

https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/optimistic_rollups/
https://medium.com/plasma-group/introducing-the-ovm-db253287af50
https://www.binance.vision/blockchain/what-is-ethereum-plasma
https://medium.com/matter-labs/optimistic-vs-zk-rollup-deep-dive-ea141e71e075
https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/zk-rollups/
https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/plasma/
https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/state-channels/
https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/payment-channels/
https://vitalik.ca/general/2019/08/28/hybrid_layer_2.html
https://medium.com/plasma-group/plapps-and-predicates-understanding-the-generalized-plasma-architecture-fc171b25741
https://www.learnplasma.org/en/learn/framework.html
https://wiki.polkadot.network/docs/en/learn-parachains
https://github.com/staketechnologies/Plasm