Era Swap Network White Paper

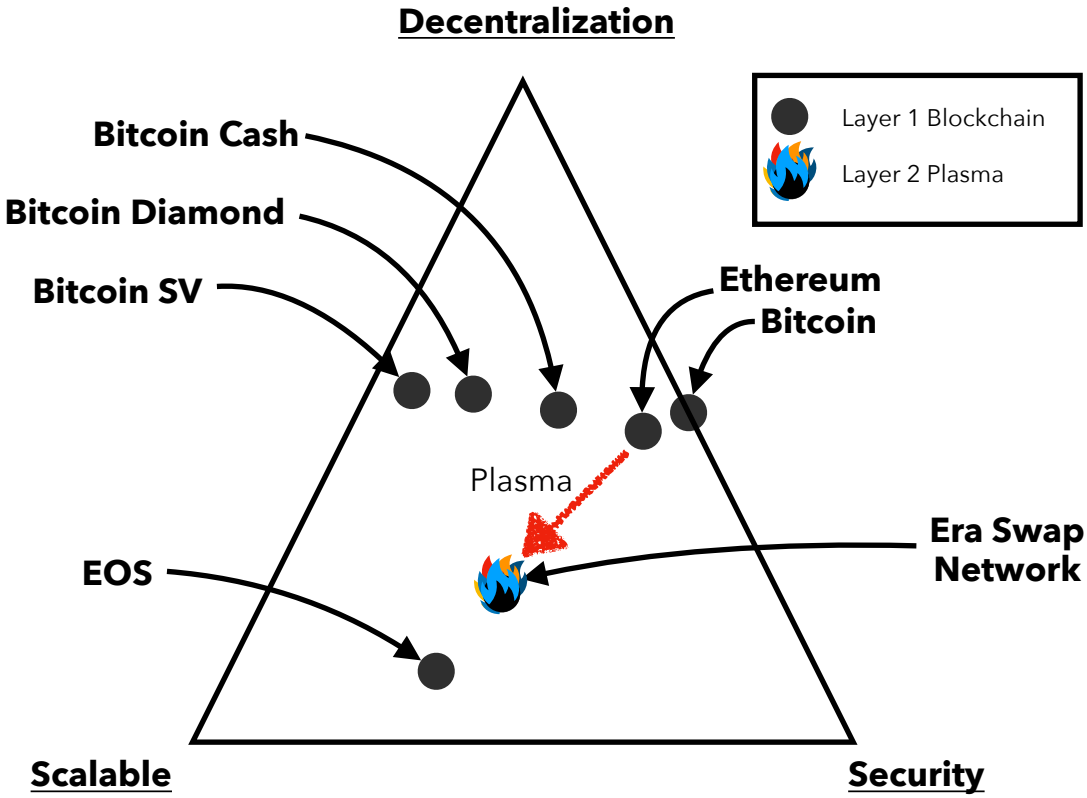
[Version 0.6.5 - Last updated on 11 May 2020]

Abstract

The early smart contracts of Era Swap Ecosystem like TimeAlly, Newly Released Tokens, Assurance, BetDeEx of Era Swap Ecosystem, are deployed on Ethereum mainnet. These smart contracts are finance-oriented (DeFi), i.e. most of the transactions are about spending or earning of Era Swap tokens which made paying the gas fees somewhat intuitive to the user just like withdrawal charges in bank or paying tax while purchasing burgers. But the charges are in Ether, which is required in addition to Era Swap tokens to use the ĐApps of Era Swap Ecosystem and it only makes a new user experience complex stuff. Also, transactions that are not token oriented like adding a nominee or appointee voting also needs considerable amount of gas fees to be charged (that too in Ether) which makes non-finance ĐApps very costly and it fails to attract users from the centralised counterparts. As more Era Swap Token Utility platform ideas kept appending to the Era Swap Main Whitepaper, more non-financial transaction situations arise like updating status, sending a message, resolving a dispute and so on. Paying extensively for such actions in another currency every time and waiting for the transaction to be included in a block and then waiting for enough block confirmations due to potential chain re-organizations is counter-intuitive to existing free solutions like Facebook, Gmail. This is the main barrier that is stopping Web 3.0 from coming to the mainstream.

As alternatives to Ethereum, there are few other smart contract development platforms that propose their own separate blockchain that features for higher transaction throughput, but they compromise on decentralization for improving transaction speeds. Moreover, the ecosystem tools are most advancing in Ethereum than any other platform due to the massive developer community.

With Era Swap Network, the team aims to achieve scalability, speed and low-cost transactions for Era Swap Ecosystem (which is currently not feasible on Ethereum mainnet), without compromising much on trustless asset security of Era Swap Tokens for community users.



Introduction to Era Swap Network

Era Swap Network (ESN) aims to solve the above-mentioned problems faced by Era Swap Ecosystem users by building a PoS-based side-blockchain on top of Ethereum blockchain using the Plasma Framework.

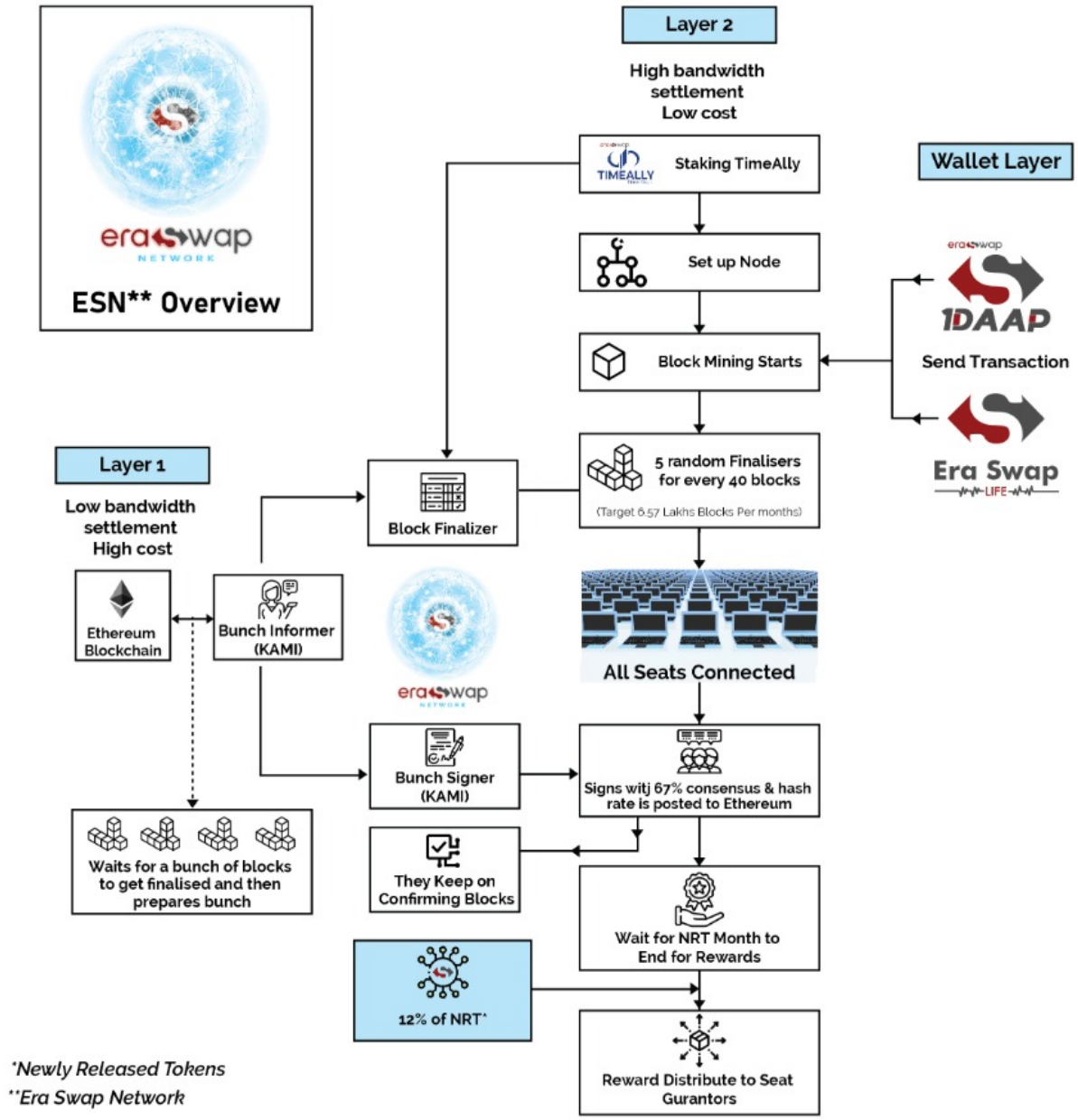
Era Swap Network leverages the Decentralisation and Security of Ethereum and the Scalability acheived in the side-chain, this solves the distributed blockchain trilema for Era Swap Ecosystem.

Currently, Etherem can do roughly 15 to 20 transactions per second and all the smart contracts including Era Swap DApps that are deployed on Ethereum manage to work with it. While in Era Swap Network, about 200 transactions per second are possible when maxed out. This gives a huge room for transactions (over 10 million per day) which is nice for Era Swap Ecosystem. In future, whenever Era Swap Ecosystem requires more capacity, it can be acheived using sharding. This is discussed in the last section.

Era Swap Network consists of **Bunches** of **Blocks** of Era Swap Ecosystem **Transactions**. A miner in ESN produces blocks, and collection of these blocks are selected and a merkle tree is created. The root of the merkle tree is submitted to the ESN Plasma Smart Contract on Ethereum mainnet. This way, all the transactions happening on Era Swap Network are fingerprinted to the Ethereum chain.

Overview Diagram

Following is a basic overview of elements in Era Swap Network.



To onboard new seats on every node the cost of every POS seat will be increasing at the rate of 0.1% based on Quadratic methodology

# of seats	Total cost All seats in ES in TimeAlly	nth seat cost in ES	Premium corresponding to nth seat	Premium %
1.000	170000.000	170000.000	0.000	0.00%
2.000	340170.000	170170.000	170.000	0.10%
n	170000(n + (n(n-1)/2000)	170000*(1+((n-1)/1000))	170000*(n-1)/1000	(n-1)/10%

Era Swap Decentralised Ecosystem

Following platforms are to be developed:

1. **Era Swap Token Contract** (adapted ERC20 on Ethereum)
   The original asset will lie on Ethereum to avoid loss due to any kind of failure in ESN.

2. **Plasma Manager Contract** (on Ethereum)
   To store ESN bunch headers on Ethereum.

3. **Reverse Plasma Manager Contract** (on ESN)
   Bridge to convert ES to ES native and ES native to ES. User deposits ES on Mainnet Plasma, gives proof on ESN and gets ES native credited to their account in a decentralised way.

4. **NRT Manager Contract** (on ESN)
   This contract manages the token release as per Era Swap Whitepaper.

5. **Era Swap Wallet** (Phone App for managing ESs and ES natives)
   Secure wallet to store multiple private keys in it, mainly for managing ES and ES native, sending ES or ES native, also for quick and easy buzcafe payments.

6. **TimeAlly** (on ESN)
   Vesting contract of Era Swap Ecosystem.

7. **SAP** (on ESN)
   Systematic Accumulation Plan for Era Swap Tokens.

8. **PET** (on ESN)
   Personal Era Swap Teller for Era Swap Tokens.

9. **DaySwappers** (on ESN)
   KYC manager for platform. For easily distributing rewards to tree referries.

10. **TimeSwappers** (on ESN)
    Freelance market place with decentralised dispute management.

11. **SwappersWall** (on ESN)
    Decentralised social networking with power tokens.

12. **BuzCafe** (on ESN)
    Listing of shops and finding shops easily and quick payment.

13. **BetDeEx** (on ESN)
    Decentralised bet proposals, bettings and results.

14. **DateSwappers** (on ESN)
    Meeting ensured using cryptography.

15. KYCDApp

16. **ComputeEx** (centralised way)
    Exchange assets.

17. **Era Swap Academy** (on ESN / centralised way)
    Learn. Loop. Leap. How to implement ES Academy is not clear. One idea is if content is constantly being modified, then subscription expired people will only have the hash of old content while new content hash is only available to people who have done dayswapper KYC and paid for the course. Dayswapper KYC is required because this way people won't share their private keys to someone else.

18. **Value of Farmers** (tbd)
    Land Registry will be recorded. And the exchange of farming commodities produced by farmers in VoF can be deposited to warehouses where the depositors will get ERC721 equivalent tokens for their commodities (based on unique tagging).

19. **DeGameStation** (on ESN)
    Decentralised Gaming Station. Games in which players take turns can be written in Smart Contract. Games like Chess, Poker, 3 Patti can be developed. Users can come to DeGameStation and join an open game or start a new game and wait for other players to join.

20. RendingDApp

21. PoolinDApp

22. CureDApp
    Medical History on Blockchain

Era Swap Network :: Specification

Era Swap Network (ESN) will be a seperate EVM-compatible sidechain attached to Ethereum blockchain as it's parent chain using Plasma Framework. The idea behind plasma framework is to avoid high transaction fees and high transaction confirmation times on Ethereum mainnet by instead doing all the ecosystem transactions off-chain and only post a small information to an Ethereum Smart Contract which would represent hash of plenty of ecosystem transactions. Also, to feature movement of Era Swap Tokens from Ethereum blockchain to ESN using cryptographic proof, reverse posting of Ethereum blocks on ESN blockchain will be implemented.

Also, submitting hash of each ESN blocks to ESN Plasma Smart Contract on Ethereum would force ESN to have a block time equal to or more than Ethereum's 15 second time as well as it would be very much costly to post lot of hashes to an Ethereum Smart Contract. This is why, merkle root of hashes of bunch of blocks would instead be submitted to ESN Plasma Smart Contact on Ethereum. There are more rewards for submitting a larger bunch / delayed.

Era Swap Network Validator nodes form the *Era Swap Network* that create blocks with PoS consensus on along with the guardian *Kami* to protect the bridge between *Era Swap Network* and *Ethereum Network*. Era Swap is imposing a strict validator node count limit to 100 nodes because every node is given a fixed amount of *Kami bonous* every month in Era Swap Tokens.

TimeAlly staking (not TSGAP, PET) can be used by staker to claim PoS seats for themselves or for others, which means it is possible for stakers to delegate their staking power to a responsible node according to them. If more than one seats are being registered, the cost PoS seats keep increasing, this will be elaborated in next section.

High Level Actors Involved

These are the actors that appear to a layman user.

TimeAlly Stakers

These are users who have some of their Era Swap Tokens staked in TimeAlly contract. TimeAlly stakings can claim PoS seats which can be used to get validator status or delegate seats to others.

Validator Nodes

It is possible for anyone to run an validator node but to become a validator and produce blocks to earn rewards, at least one PoS seat is needed (which can be claimed by TimeAlly stakers). Validator Nodes are also responsible for posting hashes to Ethereum Network. Validator Node contains ESN Node and Kami inside it.

Era Swap Users

Users who use dApps of Era Swap Ecosystem using their web browser or through an app on their phone.

Low Level Actors Involved

These are the actors in the underlying validator node.

Era Swap Network Node

This is an EVM-compatible node with consensus acheived with PoS Smart Contracts. For a node operator to get chance to propose a block, they have to stake tokens in TimeAlly and claim one or multiple PoS seats.

Every slab (40 blocks), 5 seats are selected pseudo-randomly from all the seats. Holders of these seats take turns to propose a block which gets checked by all the nodes and accepted if it's valid. If the node doesn't propose a block in allowed time, the next seat gets the turn to propose the block. After finish of the slab, new seats are selected randomly and process follows similarly. Penalty of 70,000 ES stakes burn is given if a network split occurs because of the node not producing a block. Also, if a node authors 2 different blocks in one chance, penalty of 70,000 ES stakes burn.

Block Proposer receives a Block Proposer Reward for every block they propose and these rewards can be used to claim actual ES tokens being released from next month NRT.

Kami - The Guardian of ESN

Technically, this is a background process that runs with the ESN node. The ESN node checks transactions upto an EVM context, while this is something more. A Kami looks after the proper functioning of the ESN. It keeps a very closer look on the ESN for any kind of attack taking place. If it senses one, it's guardian form get's activated and it does everything it can to prevent attack from happening.

Responsibilities of a Kami:

1. Post merkle roots from ESN to Ethereum. This task requires hold of some amount of Ether with Kami. On successful bunch submission to Ethereum Smart Contract, a Bunch Submission Reward is awarded to drive this task. The reward can be used to claim actual ES after NRT release.
2. Post merkle roots from Ethereum to ESN. Since, Ethereum is PoW based, there is a possibility for reorgs in the Ethereum blockchain. All the Kamis check if something like this is happening and update the longest chain merkle roots in ESN. This task does not cost anything, hence no reward is given.

3. Maintain proper consensus of ESN. Sometimes when some specific validator nodes act maliciously, ESN can be affected. Kamis detect any such sort of issue, and with consensus of other kamis, the malicious validator seats is suspended.

4. Check of attacks and prevent them. In times of attack, a Kami increases the security and tries as much as possible to stop the attacker's attempts to take the network down. In case of a transaction spamming attack, Kami recognizes sudden increase in transactions and counters with increased minimum gas price to drain attacker's wallet faster. In case of a theft transaction, the kamis in the validator nodes can take decision to rollback the blockchain with consensus to a block where the hack didn't take place and fork out with a clean version.

5. Give remote control access to the owner of the node. Owners can control the node from their mobile phone. The owner is authenticated by the Kami using Elliptic curve cryptography.

Quadratic Cost for PoS seats

To minimize centralization of plenty of seats in one node, we introduce a quadratic scheme in which cost of a PoS seat in a node keeps increasing.

Formula

Consider that a node has *m* number of seats already and wants to register the $(m+1)^{th}$ seat. Then the cost of the $(m+1)^{th}$ seat would be: *base_seat_cost * (1 + m / 1000)*.

Example

If a node want's to buy *n* number of seats in one go, then the cost calculation is done as follows:

Total cost = Cost of 1st seat + Cost of 2nd Seat + … + Cost of nth seat

*Total cost = base_seat_cost * (1 + 0 / 1000) + base_seat_cost * (1 + 1 / 1000) + … + base_seat_cost * (1 + (n - 1) / 1000)*

Total cost = base_seat_cost [n + (n(n-1)/2)/1000]

*Total cost = base_seat_cost * [n^2 + 1999n] / 2000*

Guarantor Function of TimeAlly

This is a delegation method which will be implemented in the redeployed TimeAlly (ESN edition). As of Ethereum deployed TimeAlly, a staker can use their stakings to guarantee (up to 50%) their own TimeAlly loans. In the new version of TimeAlly, a staker can link their stakings to give guarantee (up to 100%) of their stakings (for every NRT month) to another contract. Doing so, some credits are generated in the other contract (curators, vof, renting, …, etc) which can be used to perform critical and honest tasks for

Era Swap Ecosystem. A part of staking that is used to provide guarantee to one contract cannot be double guaranteed to other contract again.

Here, Guarantor Function of TimeAlly is used to register seats for block producer consensus in Era Swap Network. Also, if guarantee is misused by doing some malicious task, the contract can send a negative signal to TimeAlly and then the TimeAlly Smart Contract burns the staking linked to the guarantee or it arranges for a recovery option which might be required by some contracts like RentingDApp.

Gurantoor Pooling in ESN

In Era Swap Network, if stakers cannot run their node, they can guarantee their stakes to a node runner they trust which helps the node runner to register more seats and earn high profit which will be distributed back to gurantors through Smart Contract. A node can have multiple staker guaranting, and this can increase number of seats but quadratic cost will be applied. When the final profit received after NRT is released, the node runner keeps it's predefined cut and rest rewards share is distributed to guarantors in proportion of their guarantee.

Important to note: If the node is caught doing any malpractices, for example, to create a double spend (by proposing two different blocks for same height), applicable amount of stakes of the supporters will be burned in proportion of their guarantee. Hence, it is the responsibility of stakers to only pool with nodes whose owner is trustable or has a good standing to minimise chance of malpractice or run their own node.

NRT Rewards Allocation

The task that requires an effort (financial or moral), there should be some benefit available high enough to drive the desired effort.

Kami Bonus

A sponsorship amount of 1500 ES each NRT month is given for only top 100 wallet address as per seats (first come first serve) participating in Era Swap Network with at least one seat on producing at least one block. This is given from the 7% Bucket under Ecosystem Maintainance.

Block Finaliser Reward

The effort done here is the uptime of the node, that makes the Era Swap Network more secure as well as staking some ES (for which user is receives TimeAlly reward). Reward is given as per calculation from Block Finalizer NRT 2.5% as well as from the remaining of 7% Bucket under Ecosystem Maintainance (after paying Kami Bonus and Informer Reward). The reward depends on number of blocks mined, which depends on number of seats.

Informer Reward

Since, ESN and Ethereum are two separate blockchains, to move information from one blockchain to other requires a financial effort. This effort is considerable from ESN to Ethereum while less for Ethereum to ESN. This work is done by the network of Kami's (who are funded by stakers). An information update proposal needs signatures of at least 66% of seats and then only it will be accepted by Smart Contracts. A validator node that acts as an Informer has to create a bunch proposal and ask other kamis in validator nodes for their signatures on the bunch. If at least 66% signatures (by seats) are not present, then the Plasma Contract deployed on ethereum will not accept it and the transaction will fail and most of the gas sent might be consumed.

To compensate the effort as well as honour the initiative of informer, the informers are rewarded Informer Reward proportional to the number of blocks included in the bunch. This reward is given from 7% Bucket under Ecosystem Maintainance. The reward to a node depends on the bunches submitted.

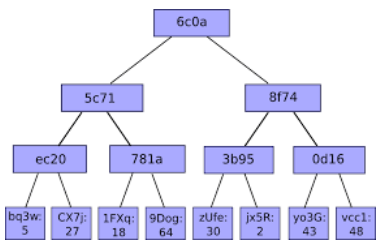
Signer Reward

When an informer creates bunch proposal, it asks to kamis of other validator nodes with seats for their signatures. When Kamis receive such request, they verify the information on it and place their signature and forward it back. Since, there is an Informer reward that goes to the informer, the Signer might refuse to sign and maliciously. To prevent this from happening and instead also give benefit to the signer through informer, a signer reward is given to all the signatures that have been included by informers in the bunch proposal sent to Plasma Smart Contract on Ethereum. Though it is possible that, signatures of stakers with more seats will be preferred since their one signature has more weightage. This reward is given from the 2.5% Signer NRT bucket. Actual reward to a node depends on number of signatures the node provider vs total signatures.

Bunch Structure

A **Bunch Structure** in Smart Contract will consist of the following:

- Start Block Number: It is the number of first ESN block in the bunch.
- Bunch Depth: It is Merkle Tree depth of blocks in the bunch. As shown in the figure, every level deep we go, 2 more nodes get added. Here, the bunch depth is 3, hence there would be 8 blocks in the bunch. And if we would draw upto bunch depth is 10, there would be 1024 blocks in the bunch. Bunch depth of Bunches on ESN Plasma Contract is designed to be variable. During the initial phases of ESN, bunch depth would be high, for e.g. 15, to avoid ether expenditure and would be decreased in due course of time.



- Transactions Mega Root: This value is the merkle root of all the transaction roots in the bunch. This is used by Smart Contract to verify that a transaction was sent on the chain.
- Receipts Mega Root: This value is the merkle root of all the receipt roots in the bunch. This is used to verify that the transaction execution was successful.

Converting ES-ERC20 to ES-Na

On Ethereum Blockchain, the first class cryptocurrency is ETH and rest other tokens managed by smart contracts are second class. On ESN, there is an advancement to have Era Swaps as the first class cryptocurrency. This cryptocurrency will feature better user experience and to differenciate it from the classic ERC20 Era Swaps, it will be called as Era Swap Natives (ES-Na). According to the Era Swap Whitepaper, maximum 910 crores (9.1 Million) ES will exist which will be slowly released in circulation every month.

Era Swaps will exist as ES-ERC20 as well as in form of ES-Na. One of these can be exchanged for the other at 1:1 ratio.

Following is how user will convert ES-ERC20 to ES-Na:

1. User will send their tokens to a Deposit Smart Contract address.
2. On transaction confirmation, a cryptographic proof will be generated by user's computer automatically (which is like a receipt of the deposit). To generate a proof, user's computer by fetches all the transactions in the Ethereum Block in which the transaction was confirmed and it constructs a Transaction Patricia Merkle Proof which can cryptographically prove that user's transaction was indeed included in the block and the Receipts Patricia Merkle Proof to confirm that the user's transaction was successful.
3. User will submit the generated proof to a Smart Contract on ESN, which would send Era Swap Native tokens to user's wallet address. Though, user will have to wait for the Etheruem block roots to be posted to ESN after waiting for confirmations which would take about 3 minutes. Once, it's done user's proofs will be accepted and will receive exact amount of ES-Na on ESN.

This process will be made user friendly by UI/UX engineering on the front-end part.

Converting ES-Na to ES-ERC20

Following is how user will convert ES-Na to ES-ERC20:

1. User has to send their ES-Na to a deposit contract on ESN.
2. Just like in previous case, a cryptographic proof will be generated by user's computer automatically. ES-Na being first class cryptocurrency on ESN, Transaction

Patricia Merkle Proof is enough to prove that user's transaction was indeed included in the block. Another thing which will be generated is the block inclusion proof in the bunch.

3. User will have to wait for the bunch to be posted to the Ethereum Plasma Contract by somebody else or user can choose to pay Gas fee and post the bunch roots themselves.

4. Once the bunch (that includes the ESN block that includes user's transaction) is posted to Plasma Contract on Ethereum, user can send the proof to the Plasma Smart Contract to receive ES-ERC20 tokens back.

Exit Game

ESN is based on the Plasma Model, when failure of sidechain occurs or the chain halts due to all the nodes shutdown, users can hard exit their funds directly from the Plasma Smart Contract on Ethereum by giving a Proof of Holdings. This has a very less possibility since there are multiple staker nodes.

Old ES Tokens swapping with New ES Tokens

The old ES Tokens will be valueless as those tokens will not be accepted in ESN because of NRT and TimeAlly contracts on mainnet which is causing high gas to users, hence reducing interactions. Also, KYC will be used to check mischief mongers on suspicious transactions done in the old ES Tokens contract. Below is the strategy for swapping tokens:

TimeAlly and TSGAP

Majority of Era Swap Community have participated in TimeAlly Smart Contract in which their tokens are locked for certain period of time until which they cannot move them. Such holders will automatically receive TimeAlly stakings of specific durations from the operator during initialisation of ESN.

Liquid Tokens

Holders of Liquid Era Swap Tokens have to transfer the old tokens to a specified ethereum wallet address managed by team. Following that, team will audit the token source of the holder (to eliminate exchange of stolen tokens) and send new tokens back to the wallet address.

Post-Genesis Token Return Program

Primary asset holding of Era Swap tokens will exist on Ethereum blockchain as an ERC20 compatible standard due to the highly decentralised nature of the blockchain. Similar to how users deposit tokens to an cryptocurrency exchange for trading and then withdraw

the tokens back, users will deposit tokens to ESN Contract to enter Era Swap Ecosystem and they can withdraw it back from ESN Contract for exiting from ecosystem network.

To manage liquidity, following genesis structure will be followed:

Holder	ES-ERC20	ES-Na
Team Wallet	117 Crore (Circulating Supply)	0
Locked in Smart Contract	793 Crore (pending NRT releases)	910 Crore

Though it looks like there are 910 * 2 = 1820 Crore ES, but the cryptographic design secures that at any point of time at least a total of 910 Crore ES (ES-ERC20 + ES-Na) will be locked. To unlock ES-Na on ESN, equal amount of ES-ERC20 have to be locked on Ethereum and vice-versa.

910 Crore ES-ERC20 will be issued by ERC20 smart contract on Ethereum Blockchain, out of which the entire circulating supply (including liquid and TimeAlly holdings) of old ES will be received to a team wallet.

TimeAlly holdings of all users will be converted to ES-Na and distributed on ESN TimeAlly Smart Contract by team to the TimeAlly holders on their same wallet address.

Liquid user holdings will be sent back to the users to the wallet address from which they send back old ES tokens (because some old ES are deposited on exchange wallet address).

ES-Na will be issued in the genesis block to a ESN Manager Smart Contract address. It will manage all the deposits and withdrawls as well as NRT releases.

Attact Vectors

1. A Validator node with stakes authors a block with an invalid transaction
   Whenever a block is received, every node in ESN checks if it satisfies EVM rules. If it does not, then the block is rejected and next seat is given chance to author the block. Hence, a block producer cannot include invalid transactions while producing the block because if it did, it would only loose it's block producer reward.

2. A Validator node with stakes attempts double spend
   When a malicious node (with stakes) tries to do double spend by creating and sending 2 different blocks, this is quickly idenfied by the network of other nodes communicating with each other. Proof the the malicious activity (signatures on two blocks of same height) is shared to all the network participants and stakes corresponding to malicious node are burned.

3. A Validator node with stakes tries to predict their selection
   The validator set is randomised by a seed that includes the previous block hash

which is unknown until the block is finalised. Hence, it is extremely difficult to predict when a validator will be selected.

4. All selected validators don't produce blocks or Handover doesn't take place due to a validators refusing to sign off
   In such an event, the Kamis of all the ESN nodes, will come in consensus with each other and fork out with a new set of validators slashing stakes associated with seats of validators that caused the issue.

5. Transaction Spamming DOS on ESN
   When a Kami detects this, it will increase the minimum gas required limit. When a spam attack is done such that a Kami cannot detect it, the Kami's owners can take an initiative to increase the minimum gas fee limit from their phone.

6. Requests Spamming on Kami
   When a Kami detects unusual load from another Kami or outside, it will deny processing any anonymous requests and demand a signature authentication.

7. Validators Disappear
   If important validators disappear, the network not able to acheive 66% consensus. In such case, the Kami's will wait for a certain time for validators to reappear, else they will fork out (this process is complex) and their stakes will be slashed. To reduce chances of this from happening natuarally, there will be an attendance system where every validator's Kami will have to mark themselves present for the next slab, in case they are not, whey will not be considered in 100% until the next slab. In case there are less than 5 seats occupied, all those seats will be block producers.

Future Scope in ESN

Sharding

Once the blockchain reaches it's capacity, to increase the capacity of ESN, one more blockchain will be deployed and it will be called as a shard. Any number of shards can be added when required and the transaction speed of ESN would be sum of transaction speeds of individual shards. Cross blockchain transactions will be achieved by posting merkle roots of a shard to every other shard. Increasing shards requires more nodes taking responsibility for securing each shard by preventing malicious behavior of any other validators and it can be achieved since if ESN with one blockchain has reaches it's capacity means there would be enough community to take responsibility. Sharding in ESN will be initiated when ESN attracts lot of users, and transactions are maintained at it's peak.

Sharding can be used to horizontally scale as much as wanted. Currently, if one ESN blockchain acheives around 500 transactions in every block, then to acheive 5000 about 10 shards (including the beacon chain) will be required.

Messaging Protocol

Since Kami's can communicate with each other as well as Era Swap Users can communicate with different different Kami's, this gives a potential of the network of Kami's to also relay some messages around. Nodes can choose to participate in this, they can generate more funds.

Roadmap Planning

Since ESN is a public system, i.e. any one can enter it into it, there are chances of people exploiting the system. To avoid ESN exploitation from the bad guys, lot of checks are drafted in this whitepaper. However, during development process, it is possible that we might figure out more points to be taken care of or we might want to change entire core system (like how we shifted from PlanB to PlanC for better security). Hence changes to the road map are expected.

- ✓ ESN Blockchain from Parity.
- ✓ Data Structure for posting Merkle roots to an Ethereum smart contract.
- ✓ Logic for verifying a transaction and receipt from a mega merkle root
- ✓ Implementation of transaction verification and testing
- ✓ Logic for Bunch Verification using multiple signatures
- ○ Implementation of Dummy Bunch Verification (centralized) and testing.
- ○ Implementation of a basic Kami that asks for signatures from others and submits Bunches.
- ○ Implement Kami posting the Ethereum blocks to ESN.
- ✓ Logic for Transferring ES from one chain to other chain
- ○ Implementation of cross blockchain ES transfer contracts and testing
- ○ Create basic UI for cross blockchain transfer of tokens
- ✓ Logic for Transferring information from one chain to other chain
- ○ Implementation of Information Transfer and testing.
- ○ Implementation in Kami to stop and start Parity Ethereum.
- ✓ Logic for Node Validators Pool (Seats allocation with a dummy TimeAlly contract)
- ○ Implementation of Node Validator Seats Allocation Smart Contract and testing.
- ○ Logic for Pseudo Random Numbers Contract
- ○ Implementation of Pseudo Random Number Contract and testing.
- ✓ Logic for Block Producer Selector Smart Contract
- ○ Implementation of Block Producer Selector Smart Contract
- ✓ Logic for Block Reward Contract
- ○ Implementation of Block Reward Contract and testing.
- ✓ Logic for Transaction Permissioning Smart Contract
- ○ Implementation of Transaction Permissioning Smart Contract and testing.
- ○ Final Implementation of Bunch Verification and testing with validators.
- ○ Logic for Cross chain transfer of Bunch Signer Awards, Submission Awards, Validator Linking Awards

- ○ Implementation of Bunch Signer Awards, Submission, Validator Linking and testing.
- ✓ Upgradable Smart Contracts framework design (initially with admin control).
- ○ NRT Smart Contract Architecture Planning.
- ○ NRT Smart Contract Implementation and testing.
- ○ Replacing dummy TimeAlly with real TimeAlly contract
- ○ Implement Guarantor Function to delegate seats power
- ○ Implement Guarantor Stakes burn
- ○ Implement Guarantor rewards delivery
- ✓ ESN Nodes Monitor Framework, to see whats currently happening live with a node
- ○ Advanced ESN Monitor Framework: check more things, and send email if any malicious activity
- ○ Alpha-release of ESN Testnet
- ○ Prepare a well documented deployment guide to remove any confusion of anything
- ○ Merkle Swap UI for tokens transfer from one chain to other chain
- ○ Engineer the Merkle Swap UX for tokens transfer from one chain to other, make it world class, extremely easy for a normal user (will be done later)
- ○ Implement the Kami Consensus for efficient checkpoint commitment
- ○ Implement the Kami Consensus for ETH-ES avg rate calculation when NRT released
- ○ Design the crypto-system for Remote Control of the Kami
- ○ Implementation of Remote Control the Kami
- ○ Implement the Gas Price limit changer by Kami
- ○ Implement Attack resistance by Kami
- ○ Implement Handover Failure Handiling by Kami Consensus
- ○ Implement the Immergency Fork by Kami Consensus
- ○ Alpha Release of ESN Mainnet

Previous Plans

The Era Swap Team had identified requirement of Era Swap Network around August 2019 after the deployment of TimeAlly Smart Contract, when community members were confused with gas fee in Ether. Also, there were many cases of transactions pending for hours due to Ethereum overcrowding.

We started designing plan for Era Swap Network since then, but it has been evolved over time to better plans due to shortcommings noticed. These plans are mentioned here for showcase of research work.

Version 1 :: Centralized Operator (18 Nov 2019)

The Version 1 release of ESN plans to fulfill the requirements for political decentralisation and transparency in ĐApps of Era Swap Ecosystem using Blockchain Technology. After aquiring sufficient number of users, a version 2 construction of ESN will be feasible to enable administrative decentralization, such that the Era Swap Ecosystem will be run and managed by the Era Swap Community and will no longer require the operator to support for it's functioning.

Era Swap Network (ESN) Version 1 will be a seperate EVM-compatible sidechain attached to Ethereum blockchain as it’s parent chain. ESN will acheive security through Plasma Framework along with Proof-of-Authority consensus for faster finality. The idea behind plasma framework is to avoid high transaction fees and high transaction confirmation times on Ethereum mainnet by instead doing all the ecosystem transactions off-chain and only post a small information to an Ethereum Smart Contract which would represent hash of plenty of ecosystem transactions. Also, to feature movement of Era Swap Tokens from Ethereum blockchain to ESN using cryptographic proof, reverse plasma of Ethereum on ESN will be implemented.

Also, submitting hash of each ESN blocks to ESN Plasma Smart Contract on Ethereum would force ESN to have a block time equal to or more than Ethereum’s 15 second time as well as it would be very much costly for operator to post lot of hashes to an Ethereum Smart Contract. This is why, merkle root of hashes of bunch of blocks would instead be submitted to ESN Plasma Smart Contact on Ethereum.

Actors involved in the ESN:

1. Block Producer Nodes
   Lesser the number of nodes, quicker is the block propagation between block producers which can help quick ecosystem transactions. We find that 7 block producers hosted on different clould hosting companies and locations reduces the risk of single point of failure of Era Swap Ecosystem and facilitates 100% uptime of ĐApps. Block Producer Nodes will also be responsible to post the small infomation to the Blockchain.

2. Block Listener Nodes
   Rest of the nodes will be Block Listners which will sync new blocks produced by the block producer nodes. Plenty of public block listner nodes would be setup in various regions around the world for shorter ping time to the users of Era Swap Ecosystem. Users would submit their Era Swap Ecosystem transactions to one of these public nodes, which would relay them to rest of the Era Swap Network eventually to the block producer nodes which would finalize a new block including the user transaction.

3. Bunch Committers
   This will be an instance in the block producers which will watch for new blocks confirmed on ESN and will calculate bunch merkle roots and will submit it to ESN Plasma Smart Contract. This instance will also post hash of new ethereum blocks to ESN (after about 10 confirmations) for moving assets between both the blockchains.

4. Users
   These will be interating with ĐApps which would be connected to some public ESN nodes or they can install a block listner node themselves. They can sign and send transactions to the node which they are connected to and then that node will relay their transactions to block producer nodes who would finalise a block including their transaction.

Shortcommings

This construction being centralised chain, would be very much dependent on operator, the Era Swap Team and users would have to trust the operator. The responsibility of the uptime and hence, the costs comes directly to the operator. There was no NRT bucket allocated for Era Swap Network, which makes running nodes loss and in future there was a possibility that operator might not be able to run the nodes.

Version 2 PlanA :: Staking-based Validator Nodes (2 Dec 2019)

While development of Version 1, it was noticed that a construction is possible in which initially the operator can manage Era Swap Network as a user. And as number of users increase, the administration the Era Swap Network will be further decentralised.

ESNv1 had a simple Proof-of-Authority consensus in which had fixed validators who would be Era Swap's initial supporters. Since it was very difficult to add more validators and there was no incentive as per whitepaper for finalising blocks, any validator who would run the chain would only do that for good will for the ESN. There was no incentive to be online. This would lead to more centralisation in the future. After a presentation, a small portion of NRT was approved for Era Swap Network by the top Era Swap Token investors.

Era Swap Network (ESN) Version 2 will also be a seperate EVM-compatible sidechain attached to Ethereum blockchain using Plasma Framework as it's parent chain like the version 1. Being administratively decentralised, current Era Swap users who have enough TimeAlly stakings can become an ESN validator by applying to to a smart contract. Anyone can run an ESN node. Era Swap users approved by the validator smart contract get validator status and their node get's turn to propose blocks. they receive a Block Finaliser reward for every block they finalise. After some blocks are finalised, when someone prepares a Bunch of these blocks for submitting to the Plasma contract on ethereum mainnet (which requires signatures of at least 66% signers), they receive a Bunch Submitter reward and also the Bunch signers receive Bunch Signer reward because they signed. These rewards can be claimed for ES tokens released from the next NRT.

Actors involved in ESN:

1. Usual ESN Nodes
   Since ESN is a public blockchain, anyone can download a software and run it by following the instructions to sync with the latest blocks. A frequent user of ESN ĐApps can install ESN node and use ESN ĐApp on it. Since, the data would be queried directly from local blockchain, ĐApp experience would be very quick compared to using ĐApp on a remote blockchain node of someone else (which is more common).

2. ESN Nodes with Validator account
   Validators set in ESN is updated every 24 hours. Era Swap users with enough TimeAlly stakings can receive validator status for the next day by applying to the Validator smart contract to be in the nextValidators set. After the change time, nextValidators become current validators and all eligible validators have next 24 hours to apply and be in the list. Running an ESN Node will do this automatically, but

in case the nodes goes offline for more than 24 hours, then that node might not be in the next list.

3. Validators accounts without ESN Node
   It is possible for some Era Swap users to have enough TimeAlly Stakings to be approved as a validator but find managing an ESN node very complex. Such users can utilise other benefits of being a Validator using their smart phone or ĐApps. One important task for maintaining ESN having correct bunch roots in the Plasma Contract on Ethereum mainnet. To ensure this, the plasma contract requires signatures of 66% of the validators. There is a Bunch Signer reward given by Plasma Contract to all those validators whose signature is present on a bunch submission. So Era Swap users can sign using smartphone/laptop on Bunch Proposals which have transaction and receipt mega merkle roots matching with mega merkle roots prepared by other trusted peer validators. Also such users can become curator in Era Swap Court to judge cases and earn Curator rewards.

4. Bunch Proposal Submitters
   For ESN to process secure deposits and withdrawals between Ethereum mainnet and ESN, the mega merkle roots of ESN block bunch have to be posted on Ethereum Mainnet which has a gas fee in ETH. This gas fee is paid to Ethereum miners who keep their systems online for keeping the network secure. Any one can submit a bunch proposal which is 66%+ validator signed to the plasma contract to receive Bunch Submitter reward.

5. Era Swap Users
   To use ĐApps of Era Swap Ecosystem, it is not required to run an ESN node (like Actor #1). Once can connect their ĐApp to any of the public ESN nodes. Public ESN nodes acts like a server which find requested information in their blockchain storage and send to ĐApps on smartphones or laptops to display on their screen. Users can anytime switch between multiple peers public ESN nodes/servers from their ĐApp settings. This is Web 3.0. Different servers can have different response time depending on the capacity of the node as well as internet connection. Some fast public ESN nodes will be arranged by Era Swap initial supporters for easy Era Swap adoption for new users.

6. Era Swap Users (Not-yet KYC approved)
   Since, Not-yet KYC approved users can misuse ESN computing resources, newly joined Era Swap Users need to complete their KYC to unlock multiple features in Ecosystem. Also such users cannot deploy a Smart Contract in ESN for security purpose. We are also exploring a possibility of restricting any Not-yet KYC address to transact on ESN unless their KYC is approved and their KYC can be done by introducer whose KYC already needs to be done. This configuration can be changed with consensus from 66% validators.

Node Validator Rewards

The Node Validator NRT will be divided into following parts by the Smart Contract:

1. **Block Finaliser Reward** 70% NV NRT (by Block Reward Contract on ESN)
   When a block is finalised, the author of the block gets Block Finaliser Reward. After NRT is released, 70% of the funds from Node Validator NRT (from whitepaper) will be distributed proportionally to the holders of Block Finaliser Reward.

2. **Bunch Submitter Reward** 15% NV NRT (by Plasma Contract on Ethereum mainnet)
   When a bunch which is signed by at least 66% of signers, it can be submitted to Plasma Contract on Ethereum mainnet by anyone and this costs gas fee in ETH. As an incentive, Bunch Submitter Reward is awarded to the submitter. After NRT is released for the month, the holders of Bunch Submitter Reward can redeem it for 150 ES for each reward. Remaining ES are burned by sending to burn address (0xbbb…bbb). In case the NRT released is less than the total bounty to be given (NRT decreases every year) then ES will be proportionally distributed between Bunch Submitter Reward holders. The reward amount can be revised in future with 66% consensus from the validators.

3. **Bunch Signer Reward** 15% NV NRT (by Plasma Contract on Ethereum mainnet)
   For a bunch proposal to be accepted by plasma smart contract, 66% of validator signatures need to be present on the proposal. To decrease the waiting time between the proposal generation and acheivement of 66% of signatures on the proposal, the availability of Bunch Signers to sign on the proposal is incentivised by awarding a Bunch Signer Reward to the signers of submitted bunch proposal by Plasma Smart Contract. After NRT is released for the month, the holders of Bunch Signer Reward can redeem it for 150 ES for each reward. Remaining ES are burned by sending to burn address (0xbbb…bbb). In case the NRT released is less than the total bounty to be given (NRT decreases every year) then ES will be proportionally distributed between Bunch Submitter Reward holders. The reward amount can be revised in future with 66% consensus from the validators.

Validator Status with TimeAlly Stakings

For ESN, having around 11 Validator nodes running would be near perfect. Having nodes less than this will make it less decentralised and more validator nodes will make it difficult to maintain 4 sec block time. The enough TimeAlly Stakings amount will adjust itself every 24 hours to make the validator block producing nodes count more close to 11 for ESNv2 mainnet. If more than 11 nodes produce blocks in a day, then the TimeAlly staking requirement will increase. Similarly, if less than 11 nodes are producing blocks then TimeAlly Staking requirement will be keep reducing unless new stakers run their nodes. For the ESN testnet, it will be 3 nodes. It need to be noted that, all validators can run their nodes, but it is possible that only 50% of validators run nodes (for block

producing) and rest don't run nodes and we want count of block producers to be 11. This requirement of 11 block producers can be changed with 66% concensus from the validators.

Shortcommings

In this plan, only top stakers were able to participate in the administration of Era Swap Network while there are 1000s of Era Swap Token holders/investors who would not be able participate.

Version 2 PlanB :: Voting-based Validator Nodes (11 Mar 2020)

In the PlanA, entire TimeAlly stakers were not able to participate in decision making process and only the top stakers were, which were some signs of centralisedness. This plan focuses more on large scale participation.

Right to administation, if given to every participant of the network, it will result in inefficiencies due to current infrastructral limitations like ping time which affects decision propagation over the network. Very frequent decisions cannot be made with everyone's confirmation because it is subject to availability of everyone which might not always be guaranteed.

To secure the network without sacrificing efficiency, ESN plans to implement Delegated Proof of Stake consensus (democracy system). Instead of entire nodes population, trusted node representatives are elected by the entire nodes population for a specific tenure. Just like in democracy, there is an election tenure like, for e.g. 4 years, here, the election tenure is 7 days and when it's finished a new set of trusted representatives will be elected.

This implementation also aims to solve problems in current democrary attempted by malicious candidates like voters are bribed to vote, fake promises, vote banks.

Digital Instruments involved:

1. Ethereum-compatible crypto wallet
   An ethereum-compatible wallet generates a 160-bit wallet address which looks like `0xC8e1F3B9a0CdFceF9fFd2343B943989A22517b26`.

2. KYC hash
   A KYC id is generated for all approved physical identities (KYCs) by Era Swap Court. Just like one person can have multiple Ethereum-compatible wallets, but only one KYC hash. Users can assign a new wallet address with their existing KYC hash. Smart Contracts related to identities will store user information by KYC hashes instead of wallet addresses.

3. ESN Nodes
   Any one can run an Parity Ethereum node above version 2.6 with ESN chain spec to sync with ESN blockchain. If the account associated with this node wins the election to become validator for 1 week, then this node can also produce blocks to get block rewards. It is not required to run an ESN node.

Actors involved:

1. TimeAlly Stakers
   These are wallet addresses with some amount of ES staked in a time bound way. These addresses can either vote or become a candidate. TimeAlly Stakers are not

required to have KYC done for casting votes to prevent off-chain contact channel to such voters. Votes are casted based on total active stakings not expiring upto 2 months in the wallet address. Voting incentivises are given to ensure maximum participation in voting.

2. Candidates
   These are wallet addresses with non-zero stakings with KYC approved by Era Swap Court. Such wallet address can apply to become a Validator (similar to Member of Parliament). To become a candidate, 100 ES nominal fee has to be paid to the smart contract (to prevent just trying for fun cases) and this amount can be revised by Era Swap Court. This fee is sent to luck pool. TimeAlly Stakers will review such wallet addresses and choose to vote from their allowance (proportional to their stakes). There can be maximum 101 candidates. Whenever an election ends (every 7 days), validators are chosen among the candidate list and the candidate list is emptied and open for fresh registrations.

3. Validators
   These are the wallet addresses choosen by Era Swap community to maintain ESN. Validators run ESN node software on their computers or on cloud providers like AWS, Azure. Each validator take turns to add a block to the ESN blockchain. The order is according to the order from the election output. In case, the validator is offline, they miss their chance to propose a block and the chance goes to next one. If the validator plays malicious by signing two blocks for same height and relay different ones to different nodes to confuse the network, with consensus of entire network they are suspended as a validator. Everyone would be seeing this on the blockchain and for the next election the malicious validator won't likely receive enough votes. Validators also have to actively sign on bunch proposals.
   In initial phase of ESN, there will be 3 validators and it will increase by 2 every NRT month upto 11. This is to reduce costs for the operator in initial phase for supporting ESN. Max validators are 11 to balance the delay in block propagation to ensure 4 sec block time feasible. Though in future, this can be changed with a hard fork if required.

4. Bunch Submitters
   Bunches of ESN blocks merklize to a transaction bunch root and receipts bunch root and bunch depth. These two values need to be communicated to the Plasma Smart Contract on Ethereum mainnet. To remove responsibility of a centralised authority to submit these values to the Ethereum mainnet, this implementation allows any one to do a bunch submission with 66% signatures. This causes gas fee in ETH to submitter, so no one would want to do it and it would be only done by those who wants withdrawal of ES. This is solved by giving Bunch Submission Reward to anyone who submits a 66% signed bunch proposal to the Plasma Smart Contract.

5. Era Swap Users
   To use ĐApps of Era Swap Ecosystem, it is not required to run an ESN node (like Actor #1). Once can connect their ĐApp to any of the public ESN nodes. Public ESN nodes acts like a server which find requested information in their blockchain storage and send to ĐApps on smartphones or laptops to display on their screen. Users can anytime switch between multiple peers public ESN nodes/servers from their ĐApp settings. This is Web 3.0. Different servers can have different response time depending on the capacity of the node as well as internet connection. Some fast public ESN nodes will be arranged by Era Swap initial supporters for easy Era Swap adoption for new users.

6. Era Swap Users (Not-yet KYC approved)
   Since, Not-yet KYC approved users can misuse ESN computing resources, newly joined Era Swap Users need to complete their KYC to unlock multiple features in Ecosystem. Also such users cannot deploy a Smart Contract in ESN for security purpose. We are also exploring a possibility of restricting any Not-yet KYC address to transact on ESN unless their KYC is approved and their KYC can be done by introducer whose KYC already needs to be done. This configuration can be changed with consensus from 66% validators.

Node Validator Rewards

The Node Validator NRT will be divided into following parts by the Smart Contract:

1. Voter Reward 20% NV NRT (by Validator Contract on ESN)
   This reward is given to incentivise TimeAlly Stakers to come online each week and cast their vote and get reward. This reward increases number of votes, hence making the election more democratic.

2. Block Finaliser Reward 50% NV NRT (by Block Reward Contract on ESN)
   When a block is finalised, the author of the block gets Block Finaliser Reward. After NRT is released, 70% of the funds from Node Validator NRT (from whitepaper) will be distributed proportionally to the holders of Block Finaliser Reward.

3. Bunch Submitter Reward 15% NV NRT (by Plasma Contract on Ethereum mainnet)
   When a bunch which is signed by at least 66% of signers, it can be submitted to Plasma Contract on Ethereum mainnet by anyone and this costs gas fee in ETH. As an incentive, Bunch Submitter Reward is awarded to the submitter. After NRT is released for the month, the holders of Bunch Submitter Reward can redeem it for 150 ES for each reward. Remaining ES are burned by sending to burn address (0xbbb…bbb). In case the NRT released is less than the total bounty to be given (NRT decreases every year) then ES will be proportionally distributed between Bunch Submitter Reward holders. The reward amount can be revised in future with 66% consensus from the validators.

4. Bunch Signer Reward 15% NV NRT (by Plasma Contract on Ethereum mainnet)
   For a bunch proposal to be accepted by plasma smart contract, 66% of validator signatures need to be present on the proposal. To decrease the waiting time between the proposal generation and acheivement of 66% of signatures on the proposal, the availability of Bunch Signers to sign on the proposal is incentivised by awarding a Bunch Signer Reward to the signers of submitted bunch proposal by Plasma Smart Contract. After NRT is released for the month, the holders of Bunch Signer Reward can redeem it for 150 ES for each reward. Remaining ES are burned by sending to burn address (0xbbb…bbb). In case the NRT released is less than the total bounty to be given (NRT decreases every year) then ES will be proportionally distributed between Bunch Submitter Reward holders. The reward amount can be revised in future with 66% consensus from the validators.

5. Validator Linking Reward 5% NV NRT (by Plasma Contract on Ethereum Mainnet)
   Validators are elected on ESN but Plasma Smart Contract on Ethereum chain does not about this. It needs to be updated with latest validators. This will be done by giving receipt proof for the InitiateChange event emitted on ESN.

Shortcommings

In this plan, there are few nodes but public doesn't get opportunity to run nodes for actually administrating the network. Era Swap Network would be more decentralised if public with less stakes can also administer the network (as much as their stakes). This led us to design the current plan as it is.