



White Paper

[Version 0.3.2 - Last updated on 28 Dec 2019]



DISCLAIMER

This Whitepaper is for Era Swap Network. Its purpose is solely to provide prospective community members with information about the Era Swap Ecosystem & Era Swap Network project. This paper is for information purposes only and does not constitute and is not intended to be an offer of securities or any other financial or investment instrument in any jurisdiction.

The Developers disclaim any and all responsibility and liability to any person for any loss or damage whatsoever arising directly or indirectly from (1) reliance on any information contained in this paper, (2) any error, omission or inaccuracy in any such information, or (3) any action resulting there from

Digital Assets are extremely high-risk, speculative products. You should be aware of the risks involved and fully consider before participating in Digital assets whether it's appropriate for you. You should only participate if you are an experienced investor with sophisticated knowledge of financial markets and you fully understand the risks associated with Digital assets. We strongly advise you to take independent professional advice before making any investment or participating in any way. You should check what rules and protections apply your respective jurisdictions before investing or participating in any way. The Creators & community will not compensate you for any losses from trading, investment or participating in any way. You should read whitepaper carefully before participating and consider whether these products are right for you.

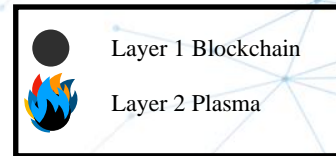


TABLE OF CONTENT

• Abstract:	04
• Introduction to Era Swap Network:	04
• Development Overview:	05
• Era Swap Utility Platform:	06
• Alpha-release Development Plan:	08
• Era Swap Network Version 1 : Specification:	09
• Bunch Structure:	10
• Converting ES-ERC20 to ES-Na and back:	10
• Conclusion:	14
• Era Swap Ecosystem	15
• Social Links	15



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 in Ether somewhat intuitive to the user (withdrawal charges in bank, paying tax while purchasing burgers) but transactions that are not token oriented like adding a nominee or appointee voting also needs Ether to be charged. 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 all day 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.

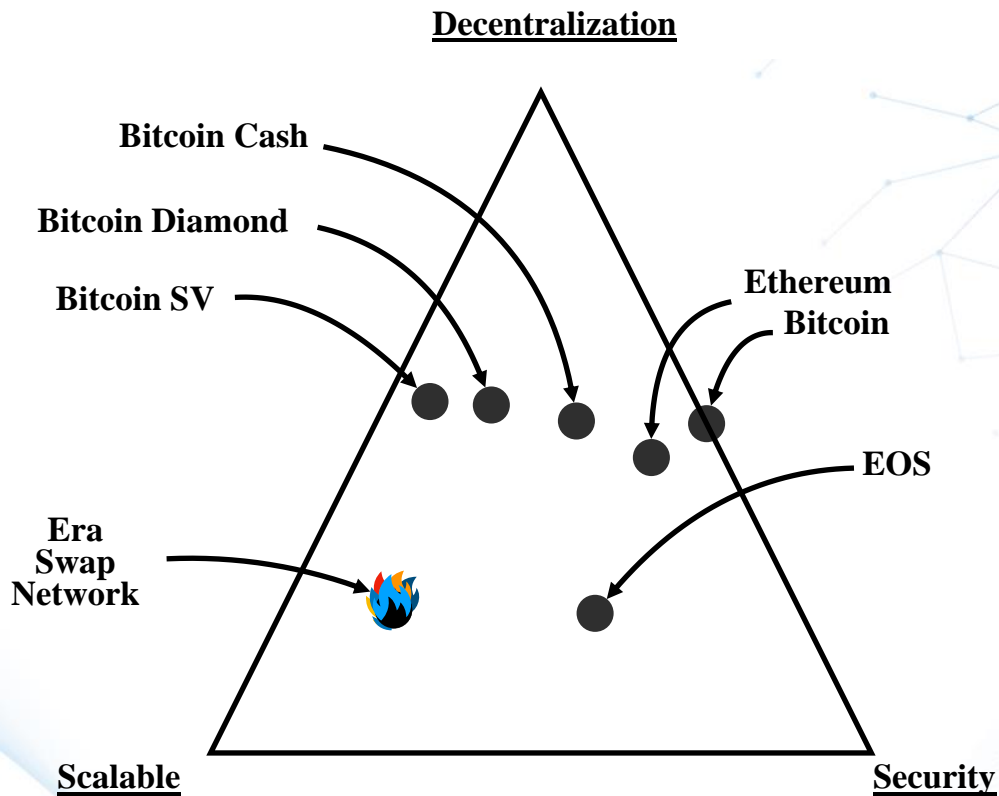
As alternatives to Ethereum, there are few other smart contract development platforms that propose their own separate blockchain that features for higher transaction throughput, but they compromise on decentralization for improving transaction speeds. Moreover, the ecosystem tools are most advancing 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 for Era Swap 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 side-blockchain on top of Ethereum blockchain using the [Plasma Framework](#).

Era Swap Network leverages the Decentralisation and Security of Ethereum and the Scalability achieved in the side-chain, this solves the distributed blockchain trilemma. In most of the other blockchains, blocks are a collection of transactions and all the transactions in one block are mined by a miner in one step. Era Swap Network will consist of **Bunches** of **Blocks** of Era Swap Ecosystem **Transactions**.



A miner mines all the blocks in a bunch consequently and will commit the bunch-root to the ESN Plasma Smart Contract on Ethereum mainnet.

Development Overview

Initially, we will start with a simple **Proof-of-Authority (PoA)** based consensus of EVM to start the development and testing of Era Swap Ecosystem Smart Contracts as quickly as possible on the test-net. We will call this as an **alpha-release of ESN test-net** and only internal developers will work with this for developing smart contracts for Era Swap Ecosystem. User's funds in a Plasma implementation with a simple consensus like PoA are still secured as already committed bunch-roots cannot be reversed.

Eventually, we want to arrive on a more control-decentralized consensus algorithm like Proof-of-Stake (PoS) probably, so that even if the chain operator shuts down their services, a single Era Swap Ecosystem user somewhere in the world can keep the ecosystem alive by running software on their system and similarly more people can join to decentralize the control further. In this PoS version, we will modify the Parity Ethereum client in such a way, that at least 50% of transaction fees collected will go to the Luck Pool of NRT Smart Contract on Ethereum mainnet and rest can be kept by miner of the blocks/bunch of blocks if they wish. After achieving such an implementation, we will release this as a **beta version** to the community for testing the software on their computers with Kovan ERC20 Era Swaps (Ethereum test-net).



Era Swap Decentralised Ecosystem

Following platforms are to be integrated:

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 Ethereum or on ESN)**
If it is possible to send ES from an ESN contract to luck pool of NRT Manager Contract on Ethereum, then it's ok otherwise, NRT Manager will need to be deployed on ESN for ability to add ES to luck pool.
5. **Era Swap Wallet (React Native 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 Ethereum or on ESN)**
On whichever chain NRT Manager is deployed, TimeAlly would be deployed on the same chain.
7. **Assurance (on Ethereum or on ESN)**
On whichever chain NRT Manager is deployed, TimeAlly would be deployed on the same chain.
8. **DaySwappers (on ESN)**
KYC manager for platform. For easily distributing rewards to tree referees.
9. **TimeSwappers (on ESN)**
Freelance market place with decentralised dispute management.



10. **SwappersWall (on ESN)**

Decentralised social networking with power tokens.

11. **BuzCafe (on ESN)**

Listing of shops and finding shops easily and quick payment.

12. **BetDeEx (on ESN)**

Decentralised Prediction proposals, prediction and results.

13. **DateSwappers (on ESN)**

Meeting ensured using cryptography.

14. **ComputeEx (on Ethereum / centralised way)**

Exchange assets.

15. **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.

16. **Value of Farmers (tbd)**

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).

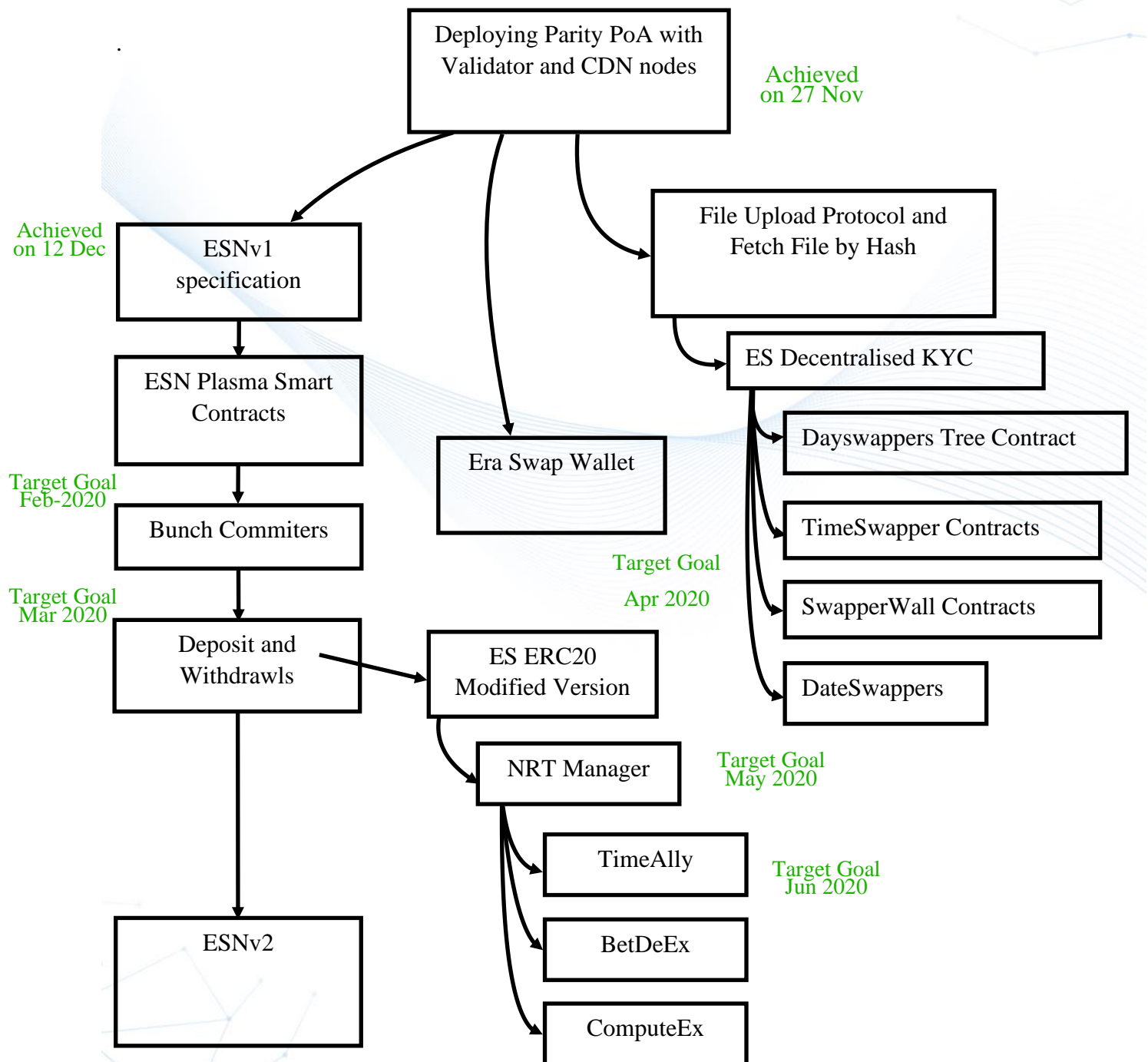
17. **DeGameStation (on ESN)**

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.



Alpha-release Development Plan

1. Deploying Parity Node customized according to Era Swap Whitepaper with PoA consensus.
2. Setting up Plasma Smart Contracts.
3. Creating a bridge for ERC20 Swap from Ethereum test-net to ESN alpha test-net.





Era Swap Network Version 1 : Specification

The Version 1 release of ESN plans to fulfill the requirements for political decentralisation and transparency in dApps of Era Swap Ecosystem using Blockchain Technology. After acquiring 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 its functioning.

Era Swap Network (ESN) Version 1 will be a separate EVM-compatible sidechain attached to Ethereum blockchain as its parent chain. ESN will achieve 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 Contract 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 hosting companies and locations reduces the risk of single point of failure of Era Swap Ecosystem and facilitates 100% uptime of dApps. Block Producer Nodes will also be responsible to post the small information to the Blockchain.

2. **Block Listener Nodes**

Rest of the nodes will be Block Listeners which will sync new blocks produced by the block producer nodes. Plenty of public block listener 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 blockchain.

4. **Users**

These will be integrating with dApps 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.

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. For e.g. If bunch depth is 3, there would be 8 blocks in the bunch and if 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, it 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.
- Timestamp: This value is the time when the bunch proposal was submitted to the smart contract. After submission, there is a challenge period before it is finalised.

Converting ES-ERC20 to ES-Na and back

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 differentiate it from the classic ERC20 Era Swaps, it will be called as Era Swap Natives (ES-Na). According to the Era Swap Whitepaper, maximum 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 give allowance to a Deposit Smart Contract, and following that call deposit method to deposit tokens to the contract.
2. On transaction confirmation, user will paste the transaction hash on a portal which will generate a Proof of Deposit string for the user. This string is generated by fetching all the transactions in the Ethereum Block and generating a Transaction Patricia Merkle Proof to 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. Using the same portal, user will submit the generated proofs to a Smart Contract on ESN, which would release funds to user. Though, user will have to wait for the Ethereum 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.

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

1. ES-Na being first class cryptocurrency, user will simply send ES-Na to a contract.
2. User will paste the transaction hash on a portal which will generate a Proof of Deposit for the user. Again ES-Na being first class cryptocurrency, 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 confirmation to the Plasma Smart Contract and once it's done, user can send the proof to the Plasma Smart Contract to receive ES-ERC20.

Hard Exit

Since the blocks are produced and transactions are validated by few block producers, it exposes a possibility for fraud by controlling the block producer nodes. Because ESN is based on the Plasma Model, when failure of sidechain occurs or the chain halts, users can hard exit their funds directly from the Plasma Smart Contract on Ethereum by giving a Proof of Holdings.

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 (New Released Tokens) and TimeAlly contracts on mainnet which is causing high gas to users, hence reducing interactions. Also, there was an event of theft of Era Swap Tokens and after consensus from majority of holders of Era Swap Tokens; it was decided to create a new contract to reverse the theft to secure the value of Era Swap Tokens of the community. 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 staking of specific durations from the operator during initialization 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. The design of the token system will be such that, it will be compatible with the future shift (modification or migration of ESN version 1) to ESN version 2, in which an entirely new blockchain setup might be required.

To manage liquidity, following genesis structure will be followed:

Holder	ES-ERC20	ES-Na
Team Wallet	1.17 billion (Circulating Supply)	0
Locked in Smart Contract	7.93 billion (pending NRT releases)	9.1 billion

Though it looks like there are $9.1 * 2 = 18.2$ Billion ES, but the cryptographic design secures that at any point of time at least a total of 9.1 billion 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.

9.1 billion 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 withdrawals as well as NRT releases.



Attack Vectors

Following are identified risks to be taken care of during development of ESN:

Network Spamming: Attacker can purchase ES from exchange and make lot of transactions between two accounts. This is solved by involving gas fees. A setting of 200 nanoES minimum gas price will be set, which can be changed as per convenience.

DDoS: Attacker can query public nodes for computationally heavy output data. This will overload the public node with requests and genuine requests might get delayed. Block producers RPC is private, so they will continue to produce blocks. To manage user's denial of service, provider in dApps need to be designed in such a way such that many public nodes will be queried a simple information (let's say latest block number) and the one which responds quickly to user will be selected.

AWS is down: To minimise this issue due to cloud provider down, there will be enough nodes on multiple cloud providers to ensure at least one block producer is alive.

User deposit double spending: User deposits ES on Ethereum, gets ES-Na on ESN. Then issue happens that there are re-orgs on ETH mainnet and user's transaction is reversed. Since ETH is not a fixed chain and as per PoW 51% attack can change the blocks. As Ethereum is now enough mature and by statistics forked blocks are at most of height 2. So it is safe to consider 15 confirmations.

Exit Game while smooth functioning: User starts a hard exit directly from Plasma Smart Contract on Ethereum, then spends his funds from the plasma chain too. To counter this, the exit game will be disabled, only when ESN halts, i.e. fails to submit block header within time the exit game starts. This is because it is difficult to mark user's funds as spent on ESN.

Vulnerability in Ecosystem Smart Contracts: Using traditional methods to deploy smart contract results in situation where if a bug is found later, it is not possible to change the code. Using a proxy construction for every ecosystem smart contract solves this problem, and changing a proxy can be given to a small committee in which 66% votes are required, this is to prevent malicious change of code due to compromising of a single account or similar scenario.

ChainID replay attacks: Using old and traditional ways to interact with dApps can cause loss to users, hence every dApp will be audited for the same.



Conclusion

Era Swap Network is an EVM-compatible sidechain attached to the Ethereum blockchain through Plasma Framework. This allows off-chain processing of Era Swap Ecosystem transactions and posting only the hash of the bunch to Ethereum. This greatly reduces the high network fee and confirmation time issues faced by the current Era Swap Ecosystem dApps deployed on Ethereum. Also, having a separate EVM-compatible blockchain tailored to Era Swap Ecosystem improves the user experience to a higher extent. Since by design, Plasma Framework makes the Era Swap Network as secure as the Ethereum Network, user's funds on the network would be secure as well.

We believe Era Swap Network will help scale dApps of Era Swap Ecosystem to onboard the increasing numbers of users.

Era Swap Ecosystem

Era Swap Ecosystem consist of multiple interlinked platforms which is powered by Era swap (ES) token, a decentralized utility token to be used on below utility platforms. Users can access the Platforms through Era Swap Life which is the Single Sign on (SSO) gateway to the one world of Era Swap Ecosystem.

Era Swap Life: <https://eraswap.life/>

- **TimeAlly DApp** -> Decentralized Token Vesting: <https://www.timeally.io/> <Beta Version>
- **BetDeEx** -> Decentralized prediction platform: <https://www.betdeex.com/> <Beta Version>
- **Swappers Wall** -> Social Time Ledgerise: <https://timeswappers.com/swapperswall> <Alpha Version>
- **TimeSwappers** -> Global P2P marketplace: <https://timeswappers.com/> <Alpha Version>
- **BuzCafe** -> Connects local P2P outlets: <https://buzcafe.com/> <Alpha Version>
- **DaySwappers** -> Unique Affiliate Program: <https://dayswappers.com/> <Alpha Version>
- **Era Swap Academy** -> E-mart for skill development: <https://eraswap.academy/> <Alpha Version>
- **Value of Farmers (VOF)** -> Farming ecosystem: <http://valueoffarmers.org/> coming soon
- **ComputeEx** -> P2P lending and borrowing: <https://computeex.net/> coming soon
- **DateSwappers** -> Next gen dating: coming soon



Smart Contract address

✚ Era Swap Token (ES)

<https://etherscan.io/address/0xef1344bdf80bef3ff4428d8bec3ee4a2cf574#code>

✚ Newly Released Token (NRT)

<https://etherscan.io/address/0x20ee679d73559e4c4b5e3b3042b61be723828d6c#code>

✚ TimeAlly DApp

<https://etherscan.io/address/0x5630ee5f247bd6b61991fbb2f117bbeb45990876#code>

✚ BetDeEx DApp

<https://etherscan.io/address/0x42225682113E6Ed3616B36B4A72BbaE376041D7c#code>

✚ TSGAP DApp

<https://etherscan.io/address/0xbad9af4db5401b7d5e8177a18c1d69c35fc03fd3#code>

White Paper

Era Swap Whitepaper: https://eraswaptoken.io/pdf/eraswap_whitepaper.pdf

Era Swap Light Paper: https://eraswaptoken.io/pdf/eraswap_lightpaper.pdf

Howey Test

Howey Test: <https://eraswaptoken.io/era-swap-howey-test-letter-august7-2018.php>

Era Swap SOCIAL LINKS

Telegram: <https://t.me/eraswap>

Twitter: <https://twitter.com/eraswaptec>

Facebook: <https://www.facebook.com/eraswap/>

Instagram: <https://www.instagram.com/eraswap/>

BitcoinTalk: <https://bitcointalk.org/index.php?topic=5025979.msg45502457>

Youtube: <https://www.youtube.com/channel/UCGCP4f5DF1W6sbCjS6y3T1g>

LinkedIn: <https://www.linkedin.com/company/eraswap/>

Reddit: <https://www.reddit.com/user/EraSwap>

Medium: <https://medium.com/@eraswap>

Tumblr: <https://eraswap.tumblr.com/>

Mix: <https://mix.com/eraswap>

Pinterest: <https://www.pinterest.com/eraswapt/>

GitHub: <https://github.com/KMPARDS/EraSwapSmartContracts>