CROSS-CHAIN FREEDOM

eywa

The most secure and decentralised cross-chain protocol

Table of contents

Introduction

Blockchain technologies are said to have three main limitations that form the blockchain trilemma – scalability, decentralization, and security. It has been postulated by Vitalik Buterin [1] that an increase in any of the three core aspects of blockchain can only be achieved as a result of the sacrifice of the other two. Illustratively, an increase in security can only be achieved via sacrifice in decentralization and scalability, while scalability demands sacrifices in decentralization and security. Such a state of affairs and the inherent limitations of the technology are the reasons for the slow propagation of decentralized networks, their challenges with security, and increasing centralization, represented by the fragmentation of the crypto market into numerous blockchains, exchanges, and protocols.

However, apart from the three pillars of the postulate, there is a fourth major factor that is impeding the adoption and propagation of blockchain as a technology among users on the market at large and as a viable system of international payments on a global scale. The lack of proper interconnections and interoperation among the various blockchains in existence is turning the decentralized environment into a major archipelago of segregated systems that compete with each other and are often so self-focused that their development vectors are contradictory.

The expansion of the cryptocurrency phenomenon onto traditional markets in the form of a new asset class is attracting greater attention to the decentralized economy as a whole. Such dynamics and movements of institutional and retail investors can best be observed within the scope of the decentralized finance market, or DeFi, which has attracted the interest of not only average users, but of entire corporations willing to capitalize on blockchain technologies as an emerging force in the world of finance.

The DeFi sector is growing rapidly and spawning a race among ecosystems. New players are regularly appearing on the market with their own products and solutions. According to analysts, the capitalization of the DeFi market was supposed to reach $100 billion by the end of 2021. However, according to Coingecko, at the end of the first quarter, that mark had already been reached with daily trading volume fluctuating in the $12-14 billion range. The capitalization of the DeFi market could probably grow multifold within a few years, given the interest of institutional investors.

Ethereum is the DeFi market leader, followed by the Binance Smart Chain, Polygon (Matic), and Huobi Ecochain, which are rapidly gaining liquidity. There are other ecosystems as well, such as Polkadot, Avalanche, Tron, Neo, Solana, Near, Terra and others.

Each ecosystem develops and promotes its own blockchains and protocols that are based on them, and each blockchain in DeFi space has its own weak points. Some boast extremely high transaction fees (for example, Ethereum), others have high degrees of centralization (like the Binance Smart Chain), while others are insufficiently liquid.

Ultimately, all the overhead and complexity falls on the users. They need to start different wallets and keep native coins in them to pay for transactions in each of the blockchains, and this is very far from a comfortable user experience.

The largest DeFi protocols, such as AAVE, Uniswap, Curve, Sushi Swap, and Cream are 3 gradually increasing the number of supported blockchains in efforts to avoid facing the high transaction fees of Ethereum, preferring instead to opt for solutions that allow their business to scale. Examples of such solutions are Polygon, Fantom, Arbitrum, Optimism and many others. All major blockchain ecosystems create bridges among each other, like Polkadot (Kusama), Ethereum, Solana, Cosmos, Terra, and Avalanche. And all of them strive to reach out beyond the boundaries of their native blockchains.

These facts suggest that the future of DeFi lies in becoming the Internet of blockchains, or, as it is also called – the Web-3.0.

Therefore, we believe that the development vector of the DeFi market is directed towards strengthening and unifying the interaction between numerous blockchains, each endowed with their own different properties and purposes.

Market Challenges

Most DeFi protocols originate on the Ethereum blockchain, but those that are based on Ethereum suffer from its inherent disadvantages of low bandwidth and high transaction fees. There have been many attempts to solve these problems. Alternative solutions are being launched that inherit the logic of Ethereum, for example the Tron chain, Binance Smart Chain, Fantom and Huobi EcoChain. They solve the problems faced by users and developers of DeFi protocols in terms of transaction costs and speeds of operation, but do so at the expense of degrees of decentralization.

There are numerous second layer protocols available as well, dubbed sidechains, rollups that use zero knowledge cryptography for solving the problem of scaling and anonymization, such as ZK-Sync, Aztec Network, Dusk network, Starknet and many others.

There are some blockchains that are decentralized enough and compatible with Ethereum, such as Matic (Polygon), Avalanche, Celo, and Near. And there are blockchains that have adopted their own development vectors, like Solana, Polkadot, Cosmos, TON or Cardano.

Such ecosystems are facing different problems, including attracting new users, teaching developers about new programming languages and approaches to product creation, or attracting liquidity. In other words, they lack a community in every sense of the word.

The ongoing processes taking place are of great interest, but developers and market participants also understand how much work needs to be done by the entire global DeFi developer community in order to create solutions tailored for the mass market. We admire the talented and intelligent people who are engaged in this noble task, as we honor their vision for the future.

Therefore, our challenge is to create an ecosystem that will become a convenient instrument in the hands of the developers of DeFi ecosystems and protocols. An instrument that would allow DeFi projects to work in synergy, leveraging the benefits and capabilities of all the best DeFi ecosystems and protocols on the market.

EYWA enables different blockchain ecosystems to mutually enrich each other in terms of liquidity, community-building, and technical integration of different DeFi projects.

Cross-chain Interoperability Landscape

We also strive to solve the problems of end users here and now, creating application functionality designed to simplify the user experience and open access to new opportunities for generating income.

The most common issues on the current DeFi market include the following:

- Poor user experience;
- Fragmentation of liquidity between multiple pools and blockchains;
- Various technology stacks that are poorly compatible with each other;
- High commissions;
- Commissions in multiple assets in cross-chain interaction;
- Low blockchain throughputs;
- Lack of ready-made tools and standardized approaches to blockchain interaction.

Oftentimes, assets that move between blockchains are illiquid and are not integrated into existing DeFi protocols. This poses a considerable challenge for both developers and users, as streamlined operations require interaction with several protocols simultaneously. As a rule, users move assets between different blockchains for very specific purposes like trading, participating in IDOs, lending, or participating in profitable farming or staking. But at the same time, they want to save on transaction costs.

In other words, end users need an end-to-end application-level solution. It is necessary to have instant cross-chain liquidity on exchanges and profitable farming tools, provide users with information in a convenient fashion, and minimize the number of transactions. All of these actions are necessary to comfortably move liquidity between different blockchains.

From the point of view of DeFi developers, using existing DeFi protocols as elements of a financial LEGO-like building block sandbox is inefficient. Developers are in need of a new toolkit that would act as a universal cross-chain communication protocol supporting heterogeneous blockchains. This is necessary in order to scale existing applications and create new decentralized apps, while focusing on developing their unique business logic, rather than solving the problems of interaction between blockchains.

Such a tool will add a new dimension to the financial LEGO-like ecosystem. The introduction of such an instrument would signify a quantum leap from playing 2D Tetris to 3D environ-ments that would be acquiring volume. Such a game would be considerably more fun to play.

The problem of interoperability between blockchains is reduced to the transfer of abstract data. Not assets, but data. In other words, the process requires the transfer of transaction hash tx and its source data content from blockchain A to blockchain B and perform the formal proof of the existence of this particular transaction with its data in the original blockchain A. The content of the transaction could even be a coded call to a 'remote' smart contract. We are interested in how interconnected blockchains can be heterogeneous and have different finality. An example of an interoperable solution within homogeneous blockchains with ultimate finality are the Cosmos and Polkadot projects, which are essentially isolated ecosystems.

Most projects solve the problems of a particular case by considering the transfer of data between blockchains as a task of transferring assets, as is the case with REN, ChainSwap, ThorChain, Anyswap, Binance Bridge, and some others.

As an exception, it is possible to note the Axelar Network and Poly network projects, which, like EYWA, provide for the possibility of making cross-chain calls between blockchains, and are not limited to working only with assets. To transfer value between blockchains, many projects, including EYWA, use synthetic assets, also called wrapped or pegged assets.

Then, the data about this action is transferred to blockchain B, where a synthetic asset sX (A) is issued for the same amount, or a similar token X (B) is sent from a wallet / smart contract.

The vulnerability inherent to this method is the "trusted oracle" problem. In order to transfer data from blockchain A to blockchain B, it is necessary to use an entity external to these blockchains – a decentralized network of oracles, or a blockchain, which acts as a network of oracles. This is important, because a malicious oracle can carry out a "man in the middle" attack by sending inaccurate data.

To solve the problem of a trusted oracle, the following approaches are used:

- Use of a centralized secure network controlled by a single owner, like in the case of the Binance Bridge;
- Development of an intermediate blockchain with BFT consensus (Byzantine Fault Tolerance), using MPC (Multi-Party Computation) based on the principles of Proof- of-Stake (PoS) or Proof-of-Authority (PoA), like in the Poly network, Axelar network, ThorChain and ChainSwap;
- Use of a hybrid approach that combines MPC and PoS, but without creating an own intermediate blockchain, using smart contracts in the public blockchain to implement the logic of PoS, like in REN.

Further classification of the relevant solutions can be carried out according to the method of storage and the source of origin of liquidity. Liquidity in the system can be custodial, and in this case, it is controlled by a single agent or a group of agents. There is also the non-custodial approach, whereby liquidity is provided and controlled by many independent players. Some specific cases will be illustrated for better understanding.

Centralization With Custodial Liquidity

This approach involves the creation of a centralized trusted oracle service or a network of oracles, which is fully controlled by the system developers and the use of centralized custodial liquidity. Obviously, it is not suitable for a decentralized system, although it is quite successfully used in practice for solving some particular problems of individual projects and has great flexibility. A good example is the Binance Bridge[2].

PoS / PoA MPC Blockchain With Custodial Liquidity

This approach involves the creation of an intermediate blockchain bridge C for transferring assets between blockchains A and B. This method can be found in ThorChain[3], Anyswap[4], the Axelar network[5].

Blockchain C is built on the basis of incoming transactions f rom connected blockchains. It stores information about the transmitted data and the consensus of nodes or oracles, each of which is a node of the network C. In the target blockchain B, as a rule, merkle- proof of the existence of a transaction in the source blockchain A (similar to Near Rainbow Bridge[6]) or proof of the existence of a record of this transaction in the chain C is produced.

Often, all funds transferred between blockchains A and B are stored distributed on special threshold wallets (the TSS threshold signature scheme is used[7]), which are generated by the network C participants, that is, they are controlled by them (ThorChain, Axelar network, Anyswap v2).

In the blockchain C, the BFT consensus is used as a consensus together with Proof-of- Stake (PoS) or Proof-of-Authority (PoA) and TSS

This method is inherently similar to the first, as it is more decentralized, but less reliable, due to the fact that PoA or PoS is used with high collateral and a small (less than a hundred) number of nodes. This makes it impossible to achieve high decentralization and system security. But, at the same time, the system becomes inflexible. The main drawback of such blockchains is that instead of working as a transport layer, they turn into a distributed custodial repository of funds managed by a small group of people.

PoA MPC Blockchain With Non-Custodial Liquidity

The Poly network[8] is based on blocks from different blockchains, while a poly chain is built as a sidechain that includes all incoming cross-chain transactions. The chain is built on the principles of BFT and uses MPC Threshold Signature Scheme. Based on this chain, proofs are produced for target blockchains.

PoS MPC Without Intermediate Blockchains With Custodial Liquidity

The REN[9] project uses REN VM – a finite state machine, producing MPC – multilateral computations with zero knowledge for calculating public and private addresses used for depositing cryptocurrencies that do not have smart contracts, such as BTC, LTC, ZEC, FIL, while none of the participants can learn any of the private keys. When a user makes a deposit to a specified address, a linked asset is created in one of the destination networks. For example, in Solana, it can be renBTC. REN plays an important role in the DeFi ecosystem by tokenizing incompatible assets.

Computations on the REN network are performed by the so-called Darknodes [10], as the network itself is not a blockchain, but seeks to achieve PoS consensus via slashing (penalties) using smart contracts hosted on the public Ethereum blockchain. To launch a node, users need to place a deposit of 100,000 REN in a smart contract. The developers of the REN network are currently in full control of it and are gradually moving towards full decentralization.[11].

It is noteworthy that the Darknodes network already has over 1,700 nodes [12], which indicates a high degree of decentralization and system reliability. The disadvantages include custodial storage of liquidity within the network. However, this task could hardly have been solved in a better fashion. The main disadvantage is the closed source code of the site, since the developers provided only part of the code and two audits of the private repositories were carried out. The network also has partially centralized management at the moment.

Roll-DPoS MPC Sidechain With Non-Custodial Liquidity

The EYWA Cross-chain Data Protocol (CDP) is a protocol for transferring data between heterogeneous blockchains, which includes EYWA Oracle Network nodes, whose operators post collateral and are financially responsible for the transmitted data. Node holders receive DPoS rewards and perform MPC calculations, forming a single BLS threshold signature, which signs the transmitted data. Each node of the network is a blockchain node, whereby the full blockchain maintains the state of the network and information on incoming cross-chain transactions. The Roll-DPoS algorithm solves the scaling problem of classic DPoS by applying the lottery principle and equal opportunities for all participants, which makes the network infinitely scalable. More on this algorithm and the structure of the EYWA Oracle Network will be revealed in the technical part of the given document.

The EYWA Cross-chain Bridge is built on the basis of the EYWA Cross-chain Data Protocol, which is necessary for the transfer of tokens between blockchains. It locks assets on the source blockchain and issues pegged “e” tokens on the target blockchain, similar to how the REN network does, but the liquidity is stored in smart contracts. It is important to note that the liquidity in the bridge is not controlled by the holders of the EYWA Oracle Network nodes, unlike in REN.

The EYWA Cross-chain Liquidity Protocol (CLP) is a decentralized cross-chain exchange distributed across various blockchains. It allows end users to work with native and synthetic assets without using intermediate entities (unlike ThorChain), perform exchanges, as well as add or remove assets to or from liquidity pools. This makes it possible to simplify the experience of end users by automating transactions with the issuance and burning of synthetic tokens during cross-chain operations. Liquidity is also non-custodial under the given protocol, since the same approaches as in any AMM DEX are applied in it.

Executive Summary

The EYWA project is an end-to-end system that allows numerous and different blockchain ecosystems to enrich each other via liquidity, community and the technical integration of various DeFi protocols. EYWA is the basic solution for building next- generation DeFi cross-chain protocols. The ecosystem that the EYWA project is building supports initiatives to narrow the gaps between different blockchains and protocols, increasing their combined synergie, and attracting new talent to the DeFi sector. It is our hope that many of the new DeFi protocols will be built using the underlying technologies of EYWA, as the core philosophy of the EYWA project is integration, communication and collaboration among the many teams working on the development of DeFi protocols, accelerating the mass adoption of blockchain technologies and cryptocurrencies.

Vision

DeFi is the future of the world's financial institutions and the global economy is witnessing the very beginning of the rapid growth of this sector. Such a derivation is highlighted by the interest in this area on the part of large venture capital funds and institutional investors, such as Andreessen Horowitz, Polychain Capital, Alameda Research and others. Significant investments in the design and development of smart blockchains and DeFi protocols are spawning a technology race.

The competition between DeFi ecosystems will eventually lead to the development of simple, streamlined financial products tailored for the mass market. These will include products that can be made available on every mobile device and will not require users to understand all of the related fundamental questions on how blockchains work, which assets to pay commissions in, which wallets to use to store these assets, where to buy them, etc.

From this point of view, EYWA is the basic solution for creating next-generation cross- chain DeFi protocols. We believe that a sufficient number of blockchains with good technologies and great prospects have already been created on the market, but it is now necessary to establish cooperation between these giants, instead of multiplying the number of entities*.

That is why our approach is blockchain agnostic, as we do not give preference to any single blockchain. We are using blockchain exclusively for the validation and safe transfer of cross-chain data in order to remain at the supersystem level**.

Using our technology, market players will be able to work not only within heterogeneous DeFi ecosystems, as before, but also between them, thus creating many new market opportunities and promising cases. Examples of such are simultaneous access to liquidity from many blockchains, cross-chain farming, distributed multi-chain DAOs, cross-chain loan protocols, cross-chain exchanges, stablecoins backed by the cryptocurrencies of different blockchains, and much more.

* "Occam's Razor" is a philosophical concept that offers not to multiply entities in logical constructions, if this is not necessary to do so.
** TSIP, the Theory of Solving Inventive Problems, speaks of supersystems, as its author – Heinrich Altshuller – studied more than forty thousand patents and formulated his theory on the basis of his analytical deductions.

The ecosystem we are building supports initiatives to bring different blockchains and protocols closer together, increasing synergies and attracting new people and new capital to the DeFi sector.

Many other DeFi protocols will be built on the basis of EYWA, as the philosophy of EYWA is integration, competition and collaboration among the many teams that are creating the DeFi sector.

Mission

The mission of the EYWA project is to unite the DeFi market's players, drive the industry to a new level of maturity, and adapt DeFi for mainstream application.

EYWA intends to make DeFi a tool that will improve the financial situations of many people around the world, reduce the number of unbanked and usher in the broader application of digital currencies as instruments for elevating national GDPs. EYWA strives to make decentralized finance easy, convenient and understandable even for beginners. This requires making the user experience as simple as possible when interacting with DeFi. EYWA is therefore creating an ecosystem that brings together the best that has been created in DeFi thus far.

EYWA is making concrete steps towards achieving this future by solving the problem of interaction between blockchains and, as a result, the fragmentation of liquidity between them. And the first step on this path is the implementation of the EYWA cross-chain data and liquidity transfer protocols.

Competitor analysis

Since the problem of liquidity fragmentation is obvious, many different teams around the world are working on its solution, and we have carefully studied their solutions.

The following is a thorough analysis of the existing competitors and protocols that allow making arbitrary cross-chain calls:

Name	Cross-chain calls between heterogeneous DeFi blockchains	Consensus	Decentralization	Liquidity	Status	Security
Poly network	+	PoA MPC chain	< 50 nodes	Non-custodial	production	hacked
Axelar network	+	DPoS MPC chain	< 100 nodes	Custodial	in development	N/A
Connext	only EVM supported blockchains	Basic consensus EVM-chains	interactive atomic swaps	Non-custodial	in production	audited
Cosmos HUB+IBC	only tendermint-based homogeneous blockchains	PoS blockchain	< 300 nodes	Non-custodial	in development	audited
Chain Bridge	+	PoA MPC blockchain agnostic	< 30 nodes	Non-custodial	in development	N/A
Chainlink Cross-Chain Interoperability Protocol (CCIP)	+	PoA MPC blockchain agnostic	~400 nodes	Non-custodial	in development	N/A
EYWA	+	Roll-DPoS MPC sidechain	infinity scalable	Non-custodial	in development	N/A

Most teams are focused on creating bridges to their own blockchains or solving the problem of interoperability in specific cases; and only a few (including EYWA) attempt to solve the general problem.

For the most part, the teams are focused on creating liquidity bridges between blockchains, allowing the exchange of identical assets.

We take a wider look at this task – we create a comprehensive solution that includes both the transport and application levels. EYWA provides a flexible infrastructure for developers of interoperable applications and a decentralized cross-chain exchange for end users.

The blockchain agnostic approach allows us to have greater flexibility in the development and management of the project's tokenomics

Here is a comparative table for 16 cross-chain projects:

Name	Cross-chain bridge	Pay tx fees in any asset	Cross-chain swap any x:y tokens	Instant add Cross-chain pools	Liquidity	Consensus	Speed 2-way bridge	Interoperability between heterogeneous DeFi blockchains	Security audit
Poly network	+	-	+ (O3swap)	-	Non-custodial	PoA MPC chain **< 50 nodes**	medium	Any	hacked
Thor Chain	+	-	+	Need use Rune	Custodial	DPoS chain **< 80 nodes**	fast	Any	hacked
Connext	+	-	+	-	Non-custodial	Basic consensus EVM- chains	slow	only EVM supported chain	audited
Near Rainbow bridge	+	-	-	-	Custodial	Basic consensus (Ethereum - PoW, Near - PoS)	slow	only Etherium, Near	audited
REN	+	-	-	-	Custodial	PoA MPC block-chain agnostic **> 1500 nodes**	fast	Any	audited, no open source
Cosmos HUB+IBC	+	-	+	-	Non-custodial	PoS chain **< 300 nodes**	fast	tendermint-based homogeneous blockchains	audited
Polygon	+	-	-	-	Custodial	PoS chain **~100 nodes**	slow	only EVM supported chain, L2	audited

Name	Cross-chain bridge	Pay tx fees in any asset	Cross-chain swap any x:y tokens	Instant add Cross-chain pools	Liquidity	Consensus	Speed 2-way bridge	Interoperability between heterogeneous DeFi blockchains	Security audit
Anyswap v2+v3	+	-	-	-	V2: Custodial V3: Non-custodial	PoA MPC blockchain agnostic (DCRM) **30 nodes**	fast	Any	hacked
Multichain	+	-	-	-	Non-custodial	PoA MPC blockchain agnostic **< 30 nodes**	fast	Any	audited
Chainswap	+	-	-	-	Non-custodial	PoA MPC blockchain agnostic **< 30 nodes**	fast	Any smarcontract chains	hacked
DFYN	-	-	-	-	Non-custodial	none	none	only EVM supported chain	n/a
Binance Bridge	+	-	-	-	Custodial	centralize service	fast	Any	audited, trusted
ChainBridge	+	-	-	-	Non-custodial	PoA MPC blockchain agnostic	fast	Any	n/a
Axelar network	+	-	-	-	Custodial	DPoS MPC chain **< 100 nodes**	n/a	Any smarcontract chains	n/a
Chainlink (CCIP)	+	-	-	-	Non-custodial	PoA MPC blockchain agnostic **~400 nodes**	n/a	Any	n/a
EYWA	+	+	+	+	Non-custodial	Roll DPoS MPC sidechain infinity scalable	fast	Any smarcontract chains	n/a

Information about the data given in the table: [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33]

We are intimidated by a clear tendency towards centralization of cross-chain solutions, as many projects are opting for an architecture that obviously cannot have a high degree of decentralization. We believe that some degree of centralization may be appropriate in the early stages of development, but the architecture should take into account the scaling of consensus to an acceptable degree of decentralization at over 1,000 participants.

The second most popular problem is custodial liquidity, whereby a transport-level solution is transformed into a distributed custodial liquidity storage operated by a small group of individuals.

The third problem is the lack of a standardized approach to the transfer of calls and liquidity between blockchains and, as a result, the potentially high complexity of integrating existing cross-chain protocols and their narrow, limited functionality, which is inconvenient for the end user.It should be noted that the cross-chain call transfer market has not yet been formed and is at a very early stage of development when large players are gradually starting to enter it.

The EYWA team is setting the task of becoming one of the leaders of this market by understanding all of its specifics and peculiarities.

Solution: EYWA protocols

EYWA is an infrastructure solution consisting of a number of core components, including the following.

Here is a comparative table for 16 cross-chain projects:

The EYWA development team is creating an application layer protocol that empowers users to experience new opportunities in DeFi.

The team is solving the so-called “last mile” problem by developing a convenient decentralized cross-chain exchange for users seeking to move assets between blockchains as part of their DeFi earning strategy. If we consider our approach from the point of view of the classification given in Section 5, EYWA can be classified as follows: Roll-DPoS MPC Sidechain With Non-Custodial Liquidity.

What is the EYWA Cross-chain Liquidity Protocol? It is a system of decentralized AMM exchanges based on various blockchains, all of which are united in a single interface.

EYWA will be providing support for various AMM models that are most suitable for different types of assets: stable pools (Curve[34]), classic pools Uniswap v2[35], v3 and Balancer v2[36]. The development team will strive to create pools that are of greatest convenience for developers, end users, and liquidity providers. This approach will ensure the availability of non-custodial liquidity in the system that will be granted by liquidity providers. They will be generating profits through such activities by relying on yield farming and receiving rewards in the EYWA token.

The EYWA Cross-chain Bridge is an integral part of our liquidity protocol. To transfer value (tokens) between blockchains, EYWA will use secured synthetic assets, called “e” tokens that are created and converted according to the mint-burn principle. We call these operations synthesis and unsynthesis. The EYWA Cross-chain Data Protocol is used to transfer arbitrary information between blockchains. By locking the original asset in one blockchain, EYWA will create its synthetic analogue in another blockchain. In the reverse operation, the synthetic asset is burned, and the original is returned to the user.

The presence of such assets allows for the rapid creation of cross-chain pools and liquidity bridges that are physically located on the same blockchain and provide fast two-way movement of assets. Thus, liquidity will be freely distributed between blockchains, concentrating where it is most profitable and promising to be applied. We will monitor the development of the industry and offer new opportunities to users to suit the dynamics of the market. This system is open, and any DeFi project will be able to create its own cross-chain pool of liquidity using our system.

Synthetic assets as a cross-chain bridge. We will be offering DeFi developers a convenient and fast means of moving their tokens to the blockchains they are interested in. There are two approaches to building a cross-chain bridge:

- Locking tokens in the source blockchain and receiving their synthetic analogues in the target blockchain. In this case, users will have one source of emission and a single tokenomics model of the project;
- Creating native tokens in each blockchain and exchanging these tokens through the bridge. In this case, the bridge will be acting as a storage medium. The peculiarity of this approach is that users will have a separate tokenomics model in each of the blockchains, but at the same time, they will be the owners of the token contract

EYWA will be taking the first approach due to its inherent flexibility and simplicity in terms of bridge maintenance.

Non-Custodial Liquidity in Cross-Chain Bridges. Liquidity stored in smart contracts as collateral for synthetic assets can be extracted either by the owners or based on a general majority vote of the EYWA DAO.

EYWA Cross-chain Data Protocol (CDP)

The EYWA Cross-chain Data Protocol will be an open, decentralized cross-chain data transfer protocol capable of working between heterogeneous blockchains. EYWA intends to make this tool available and accessible to all DeFi developers. This is the transport layer of the solution consisting of a set of smart contracts in different blockchains and a native decentralized network of oracles.

The solution will allow project teams to focus on developing the business logic of their dApps without being distracted by interoperability issues. The EYWA protocol will allow projects to link any two smart contracts located in different blockchains, thus implementing remote calls between them.

Many projects are creating their own bridges for transferring liquidity between blockchains. With EYWA, bridges are more of a special case of using the transport layer in the form of a cross-chain data transfer protocol. The EYWA Cross-chain Data Protocol consists of the EYWA Oracle Network, a decentralized oracle network, and a set of smart contracts across different blockchains.

EYWA Oracle Network

The ideology of this network is inspired by Chainlink, Ren and Horizon [37] projects. The oracle network is a sidechain that can connect with any blockchains that support smart contracts. This network publishes data about its state and is managed via smart contracts located in any suitable (fast, decentralized and cheap) public blockchain. The oracle network has a distributed consensus. By voting, oracles confirm the fact of transaction conducted in the original blockchain.

When a quorum is reached, the network records verified transaction data and cryptographic evidence to the managing blockchain and then further transfer of these transactions to the target blockchains is carried out with the help of any interested parties. Absolutely anyone can transfer these cross-chain transactions and be the owner of the EYWA Oracle Network node.

Participants earn money thanks to the incentive system embedded in the project's tokenomics. It should also be noted that in order to participate in the consensus, node holders must make a pledge – a certain amount of the project's governance tokens, which are locked in a special smart contract. It distributes rewards among node holders.

For oracle consensus security, we use a modern and ecofriendly approach to decentralization used in projects such as Tezos, Polkadot, FreeTon, IoTeX, Algorithand and Ethereum 2.0 - proof of stake with slashing mechanism.

In other words, EYWA node holders are financially responsible for the data they transmit. If the EYWA Oracle Network detects a distortion of the transmitted data, all participants who participated in this are fined.

EYWA Multichain Gasless

EYWA Multichain Gasless is a subsystem that is responsible for paying for protocol transactions in multiple blockchains. We delegate to it both the execution of user transactions and the execution of transactions between blockchains on behalf of the EYWA Oracle Network oracles. This alleviates the need for users to pay fees in various assets and allows them to choose which asset to pay all fees with. Gasless also makes it possible to compensate for transaction costs for some groups of users.

The main feature of this subsystem is that the caller has the opportunity to transmit a transaction to the blockchain at the expense of the recipient. In this case, instead of sending a transaction to the blockchain, an off chain meta-transaction is formed and signed, which is then transmitted to the relay nodes; its content and structure are verified by smart contracts and then executed In our code, we use developments of such projects as OpenGSN [38] and Gnosis Safe[39], based on the EIP-712[40] standard.

EYWA Cross-chain DAO [41][42]

To manage smart contracts of a system distributed in a variety of blockchains, we will make the decision-making system distributed and governed by all holders of the project’s governance token. To link various parts of the system together, we will use the EYWA Cross-chain Data Protocol.

Features and Benefits For liquidity providers:

Cross-chain yield farming: a liquidity provider can provide liquidity to cross-chain pools and receive a reward for this. In fact, to do this, they will need to create secured synthetic assets originating from various blockchains and add them to the liquidity pool. Cross-chain pools without impermanent losses with limited liquidity and increased profitability: unlimited liquidity is not required for the effective operation of cross-chain pools, so the offer for liquidity providers will be limited and have attractive yield.

The absence of impermanent losses is achieved due to pools structure: they will consist of different representations and analogues of the same assets, for example, a curve pool in the Matic blockchain will be as follows:

eUSDC(ETH)+eUSDC(BSC)+eUSDC(HECO)+USDC(Matic)

another example, curve pool in Binance Smart Chain:
eETH(ETH)+eETH(Matic)+eETH(Solana)+ETH(bep20)

Or a similar Uniswap v2 pool in Binance Smart Chain:
eWBTC(ETH)+BTCB(bep20)

«E»-tokens are synthetic EYWA assets issued by the EYWA bridge, backed by a collateral blocked in a smart contract in the original blockchain.

The name of the bep20 token in the Binance Smart Chain of the eUSDC(ETH) type means that it is a synthetic asset backed by the erc20 USDC token in the Ethereum blockchain. This security is stored in a special contract (we call it Portal) and can be extracted by calling the EYWA bridge – in this case, the bep20 eUSDC(ETH) token will be burned, and the user who called this operation will receive a USDC token to his wallet in the Ethereum erc20 blockchain.

For EYWA DEX end users (traders):

Cross-chain exchanges allow users to freely exchange one native token for another native token in another chain, for example, ETH for BNB or USDT (BSC) for USDC (ETH) using two or even three blockchains. This can be achieved both by using the EYWA protocol's own liquidity pools, and by aggregating liquidity pools of existing large decentralized exchanges in various blockchains

The ability to make cheap transactions by exchanging assets of «expensive» blockchains, for example, to exchange erc20 Ethereum tokens using a cheap intermediate blockchain and so-called loopback swap.

For example, the exchange can take the following form:

Ethereum: USDT(erc20) => synthesis (mint) in Polygon: eUSDT(ETH) => =>swap in Polygon: eUSDT(ETH)/eETH(ETH) => get eETH(ETH) => =>unsynthesis (burn) in Polygon: eETH(ETH) => Ethereum: ETH

The ability to make cross-chain transactions between two blockchains using a cheap and fast intermediate blockchain. For example, let's take a look at the following exchange:

A user exchanges USDC between Ethereum and Binance Smart Chain blockchains using a curve cross-chain pool in Polygon:

**Ethereum: USDC(erc20) => synthesis (mint) in Polygon: eUSDC(ETH) => swap in Polygon: eUSDC(ETH)/eUSDC(BSC)/eUSDC(HECO)/USDC(Polygon)=>
=>get eUSDC(BSC) => unsynthesis (burn) in Polygon: eUSDC(BSC) => BSC: USDC(bep20)**

It is important to note that in the previous two cases, the user has the opportunity to perform this chain of operations automatically, while paying fees with the asset he has in the original blockchain, but an experienced user can manually control this process and pay fees in the networks' native assets.

Cross-chain exchange rate: fast two-way exchange between different blockchains. Unlike many bridges (Polygon PoS bridge, Near Rainbow Bridge, Plasma, Connext), our technology makes it possible to perform operations at almost the same speed, regardless of the direction of exchange.

Compensation of transaction costs for some groups of users from the protocol's profit. For example, such a group of users can be traders who make transactions for small amounts and have a modest trading turnover.

The opportunity to receive commissions by inviting liquidity providers and traders. Improved UX for end users thanks to gas-free transactions: users will be able to pay fees in the assets they exchange, or choose a convenient asset for paying fees. A progressive fee scale for traders, depending on their trading volumes. The larger the volume, the lower the fee.

The possibility of profitable exchanges: the exchange will provide intelligent routing between liquidity pools in different chains, which searches for the optimal cross-chain exchange path.

For DeFi projects developers:

The ability for quick cross-chain integration of your protocol using the EYWA Cross-chain Data Protocol (CDP) technology.

Developers will be able to ensure the connection between their smart contracts deployed in different blockchains. In particular, they will be able to create their own bridges for liquidity, cross-chain lending, cross-chain farming and other applications

Fast cross-chain liquidity - developers will be able to move tokens of their projects between blockchains using EYWA Bridge and create their own cross-chain liquidity pools using the Cross-chain Liquidity Protocol.

The opportunity to join the EYWA developer community, take part in hackathons, receive grants from the EYWA DAO and build the future of DeFi together with us.

For stakers and decentralized networks node holders:

The ability to support the operation of the EYWA Oracle Network, to be an owner of its nodes or a staker and make money on it. For EYWA token holders - to be a part of the EYWA DAO: The ability to participate in the protocol governance by submitting proposals and participating in voting. The ability to make key decisions for the EYWA ecosystem development. Make a profit from staking and rewards for taking part in voting.

Operating principles

In this section, we will take a closer look at the technical part and the internal structure of EYWA components.

EYWA Cross-chain Data Protocol and Oracle Network

In this section, we will take a closer look at the technical part and the internal structure of EYWA components. The protocol consists of a decentralized oracle network - EYWA Oracle Network - and a set of smart contracts deployed in public blockchains. It is a transport layer and provides interoperability fulfilling the following requirements:

- Decentralized operation of the protocol with a large number of participants, protected from compromise by collusion of a narrow circle of people.
- Low cost of entering the consensus with a high cost of compromise.
- The ability to combine networks with various technological solutions and rules for validation/block formation.
- The transmitting network should not store the transferred assets — a non-custodial solution.

The increase in the cost of compromise is achieved by increasing the number of consensus participants - thousands of nodes against dozens in PoA, DPoS solutions and by dividing responsibilities between participants by introducing roles:

- **Leaders** are consensus participants who collect packets from new requests for data transfer between heterogeneous blockchains and pass them to validators for validation.
- **Validators**- validate the packets coming f rom Leaders. Working within the f ramework of the BFT consensus - Tendermint[43]- they come to a consensus on the validity of the package and confirm it by generating a multi-person signature (MPS) based on the BLS cryptographic system [44].

- **Archivists** - publish processed packets to a public, independent network to record the result of the protocol operation and ensure the availability of information.
- **Backup validators** are necessary to protect the consensus from a potential attack aimed to interfere with the functioning of the protocol.

The honesty of the participants chosen for the role is achieved by an economic benefit built on the prisoner's dilemma[45] from game theory, which states that it is more profitable for each participant to betray the attacker (even if there is a preliminary collusion) and receive a reward, rather than join the attacker and incur punishment.

The roles are randomly distributed among the network participants and assigned to them until the end of the epoch.

An epoch is a period of protocol operation that is limited in time or by the number of processed packets.

The use of the Roll-DPoS algorithm guarantees a constant turnover of participants who perform their roles in the consensus. Roll-DPoS is a scaling algorithm that eliminates the problems listed above. Based on a fair lottery (built on a verifiable random function – VRF), the choice of random network participants to perform roles eliminates the risk of collusion to influence the network by a narrow circle of intruders, since it is mathematically impossible to predict the lottery results.

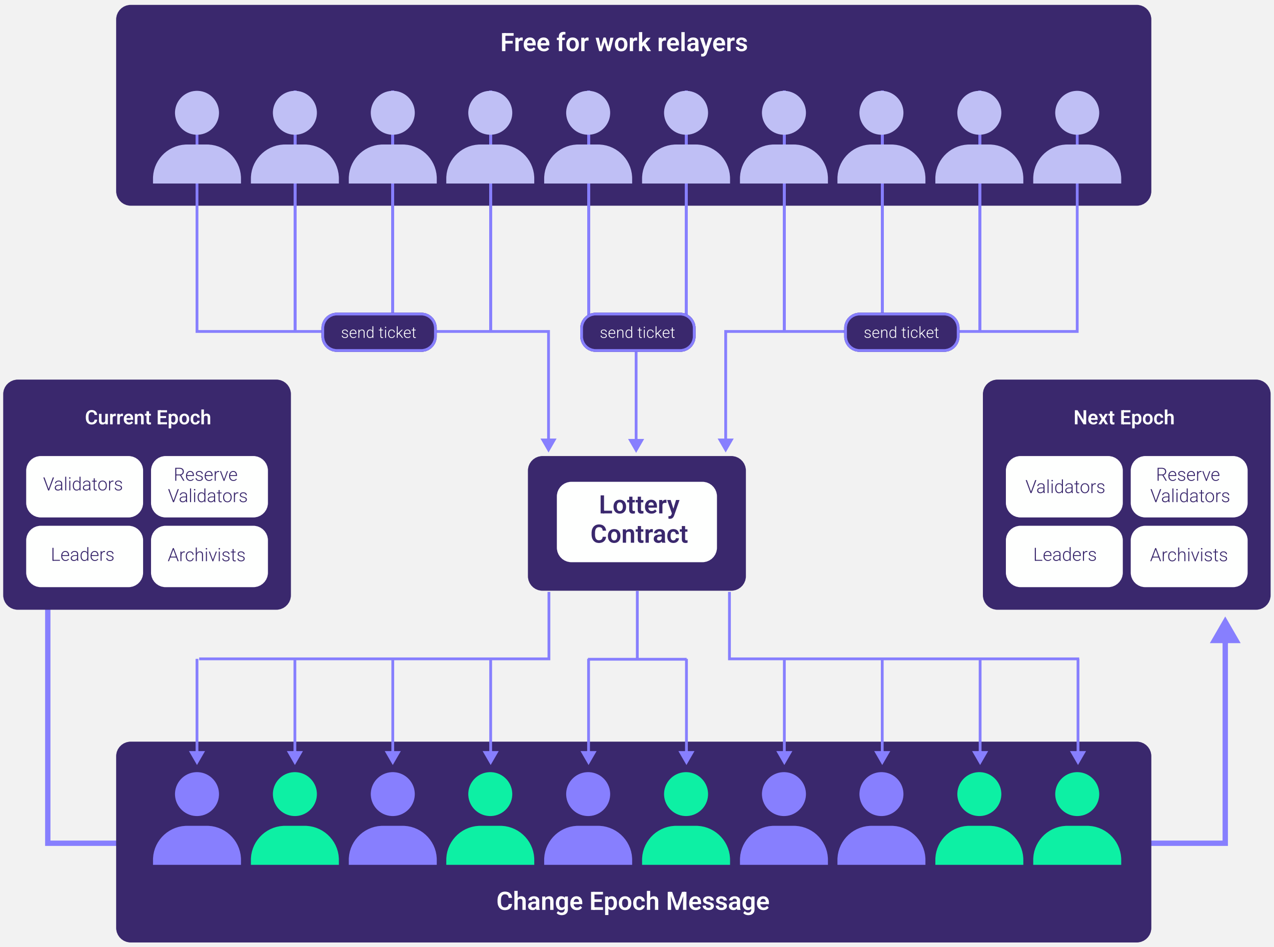
This algorithm is used in the IoTeX blockchain [46], which specializes in combining the Internet of Things (IoT) into a single blockchain, where they use RollDPoS for infinite network scaling.

The epoch change algorithm is similar to the algorithm for processing a cross-chain data transfer request, but the protocol itself acts as the source of the request, and all networks connected to the protocol are the recipient.

The EYWA Cross-chain Data Protocol keeps records and selects the participants of the epoch in a smart contract executed in an independent public blockchain, ensuring that participants of the protocol have no opportunity to influence the progress of implementation.

During the normal operation of the protocol, the leader, validators and archivist are engaged in forming a request for changing the epoch, validation and execution, but to eliminate the possibility of blocking the epoch change by validators, the role of backup validators is necessary, whose job is to force the epoch change.

For DeFi projects developers:



To organize a fair lottery, a verifiable random function (abbreviated VRF) and a starting point (seed) are used.

VRF [47] is a cryptographic primitive that can map input data to a verifiable pseudo- random output. In 1999, Mikali (founder of Algorand), Rabin and Vadhan created VRF. Currently, the VRF algorithm is used in various encryption schemes, protocols and systems.

Seed is a number, the point from which a sequence of pseudo-random numbers begins. A slight change in the starting point leads to an unpredictable change in the result of generating pseudo-random numbers.

The roles lottery for the E_N era takes place in 3 stages:

Fixing the amount of collateral for potential lottery participants. When the E_{N-3} epoch changes, the state of the network is fixed at the root of the Merkle tree, which includes all the amounts of the participants' collateral at the moment.

$Balance_i$ = (key,value) – a combination of the wallet's public key and its EYWA token balance.

CirculationSupply= $Balance_i$

CirculationSupply – the set of all non-blocked balances of the **$Balance_i$I** protocol users,

stake($Balance_i$.key, $Balance_i$.value, S)=$Stake_j$ – the function of freezing part S of the user's balance **$Balance_i$.value** and getting them a steak **$Stake_j$.**

Stake =(Balance .key, S), S ≤ Balance .value $_{jii}$

TotalStake= Stake , Stake ∈ TotalStake – the set of all $_{jj}$

stakes **$Stake_j$** from **J** consensus participants.

TotalStake ηCirculationSupply = θ – all tokens blocked for staking do not participate in the general circulation.

Collateral = 100 000 EYWA the size of the minimum stake, which guarantees the honest work of the user, can be changed by the EYWA DAO decision.

OraclesStake= $Stake_k$, ∀Stake∈$OraclesStake_k$

Stake.value ≥ Collateral, OraclesStake ⊆ TotalStake$_k$

OraclesStake – is a subset of **TotalStake**, consisting of **K** stakes of **Stake$_k$**, value participants whose value is greater than or equal to the size of the minimum **Collateral**, who have a chance of winning and the right to participate in the lottery.

During the **E$_{N-2}$** epoch any participant (**Participant$_i$**), who wants to participate in the epoch publishes a lottery ticket - **draw**(**Stake$_k$**) in the governance network. With the publication of the lottery ticket, the participant fixes the amount of his security and blocks its change until the epoch ends.

draw(Stake$_k$)=Participant$_l$

∀Participant ∈ LotteryStake, Participant ∉ OraclesStake, $_{ll}$

LotteryStake = Participant$_l$

OraclesStake ∩ LotteryStake = ∅

At the time of the **E$_{N-1}$** epoch change, the VRF result generated by the participants of the epoch is published and used as a starting point (**Seed**) for lottery tickets. The time- spaced disclosure of the starting point, fixing the amount of collateral and publishing lottery tickets is necessary to strengthen consensus by eliminating the possibility of manipulation to gain an advantage in the lottery.

Seed ∈ N — is a pseudo-random number, the result of a verifiable random number generation function.

At the time of the **E$_{N-1}$** epoch change, the acceptance of tickets for participation in the **E$_N$** epoch is completed and the list of participants is determined. Participants form collective keys and pass them to the participants of the current era to start working. The list of lottery participants who have received the right to participate in the era is determined by a weight function with priority to the participants who received the highest result during the lottery. The weight of a lottery ticket is defined as: the ratio of the hash from the key pair of the ticket owner and the lottery seed modulo the collateral of the ticket owner to the sum of all the participants' collateral.

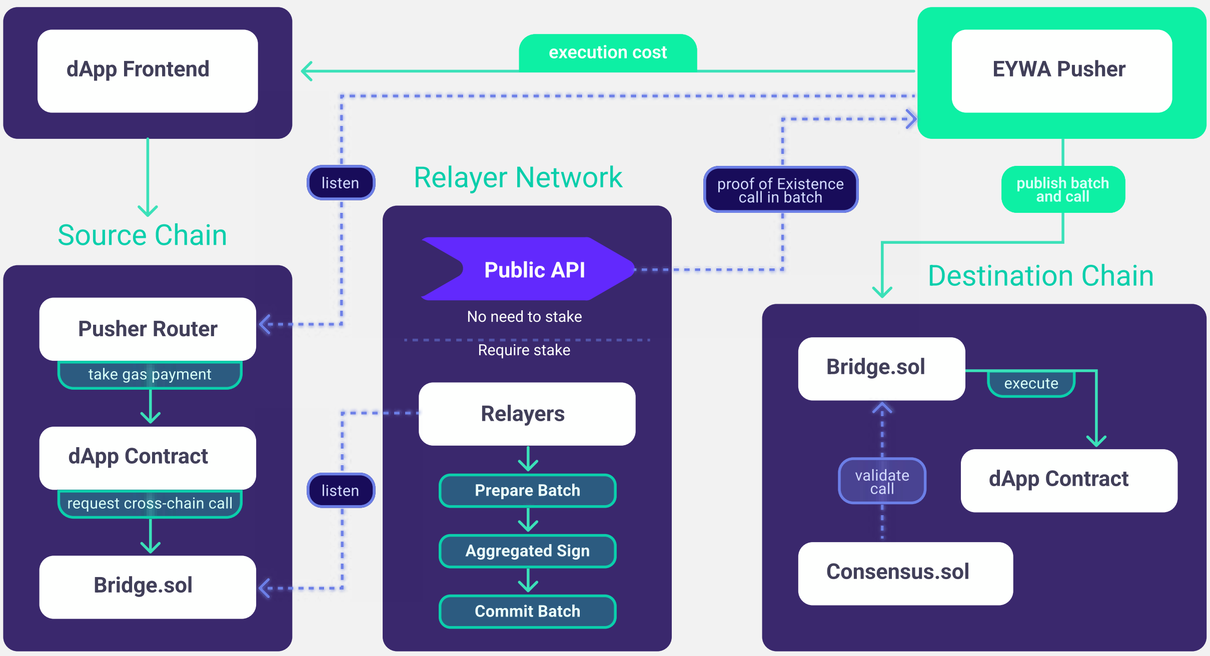
$$weight(Participant_p) = \frac{HASH(Participant_p.Key, Seed)(mod\ Participant_p.Value)}{\sum_{i=0}^{L} Participant_l.Value},$$

$$0 < weight(Participant_p) Participant_p.Value) / \sum_{i=0}^{L} Participant_l.Value,$$

Therefore, the higher the participant's deposit, the higher his chances of winning the lottery and getting into the epoch. Tickets are sorted by their result and the roles are distributed from the highest to the lowest in order of the role importance: validators, backup validators, leaders, archivists. The number of participants in each role is determined by the protocol settings.

EYWA Cross-chain Data Protocol Design

The main task of the protocol is to transfer the request of an arbitrary application X from network A to network B. Application X implements a smart contract in Network A to form and send a request to the Bridge smart contract protocol in Network A.



The epoch leader fulfills its obligations by adding a new request to the packet (batch) for subsequent validation by Validators and publication by Archivists.

After the completion of the control network block with the packet containing the request, the operation of the EYWA Oracle Network oracle network is completed. A governance network is any EVM-compatible blockchain that meets the requirements of decentralization, speed and low transaction cost, currently there are many such blockchains, we study and test them, choosing the most suitable, possible candidates include Harmony One, IoTeX, Avalanche, Celo, Polygon.

Any interested party can execute a request on network B: a client-application X, a specialized service, or a user.

To minimize the technological complexity associated with storing and managing various cryptocurrencies necessary to cover transaction costs in destination blockchains, the EYWA protocol provides the EYWA Multichain Gasless service.

The algorithm for performing a call

The step-by-step algorithm for performing a cross-chain call looks like this:

- A third-party developer's contract calls the transmitRequestV2 method in the Bridge.sol contract in the source network of the call and transmits the destination network ID, the recipient's address / contract ID, funds for payment for work (at least the amount set as the minimum payment in the protocol settings), and data for the call.
- The Bridge contract creates an OracleRequest event with the information received from the third-party developer's contract.
- Epoch leaders track events from source networks and store locally information about the call waiting for validation.
- The selected package leader (determined by the round-robin algorithm from the list of all the leaders of the epoch), determines the moment when it is necessary to form a packet and forms a packet signed with a private key. And offers the epoch validators to validate it.

- Validators accept a packet if:
  a. All pending requests and actions required by the protocol are incleded (or the packet limit defined by the general protocol settings has been reached),
  b. All the included actions are valid: there is a corresponding request in the source or the action is expected in accordance with the rules of the protocol, for example, accrual of remuneration, withdrawal of funds for compensation for work, etc.
  c. The packet is offered by the leader in the time period allotted for it,
  d. The expected archivist is assigned,
  e. The expected sequence number of the packet is set,
- Validators generate a common signature and pass the packet to the archivist for publication.
- The archivist checks the packet:
  a. The packet indicates the current epoch,
  b. The sequence number of the packet corresponds to the expected one (the next one from the last known one),
  c. All the included actions are valid: there is a corresponding request in the source or the action is expected in accordance with the rules of the protocol, for example, accrual of remuneration, withdrawal of funds for compensation for work, etc.
  d. The selected leader and archivist of the packet correspond to the expected ones (roundrobin from the serial number of the packet and the list of leaders and archivists of the current era),
  e. The leader's signature is generated from the key of the selected leader,
  f. Verifies the signature and verifies that more than $\frac{2}{3}$ of all validators were required to generate it.
- If the packet does not comply with the rules, the archivist ignores the package and waits for the next one. If the packet has passed verification, the archivist signs it with his private key and publishes it together with the signature in the protocol governance network.
- The contract in the governance network checks the received packet for compliance with the rules (similar to the archivist, but within the framework of a smart contract).
- The contract in the governance network verifies the signature of the archivist.
- The contract in the governance network adds a packet to the registry and creates a Batch event containing the package data and the archivist's signature.

- Users interested in performing actions (senders of initial requests or other persons), wait for an event to occur in the governance network and send the final calls in the destination network a transaction containing: an array of missing packets, including the current packet and the call (for execution).
- The contract of the receiving party validates the packet by analogy with the contracts in the governance network. Missing packets do not need to be checked, since the presence of a more up-to-date packet confirms the validity of the previous ones.
- The contract executes the call and returns success or error.
- In case of an error, the receiving network contract automatically creates a RequestRevertAction event, which works similarly to requestAction, but in the opposite direction to notify the source network of the error.

Types of calls and commands in the packet

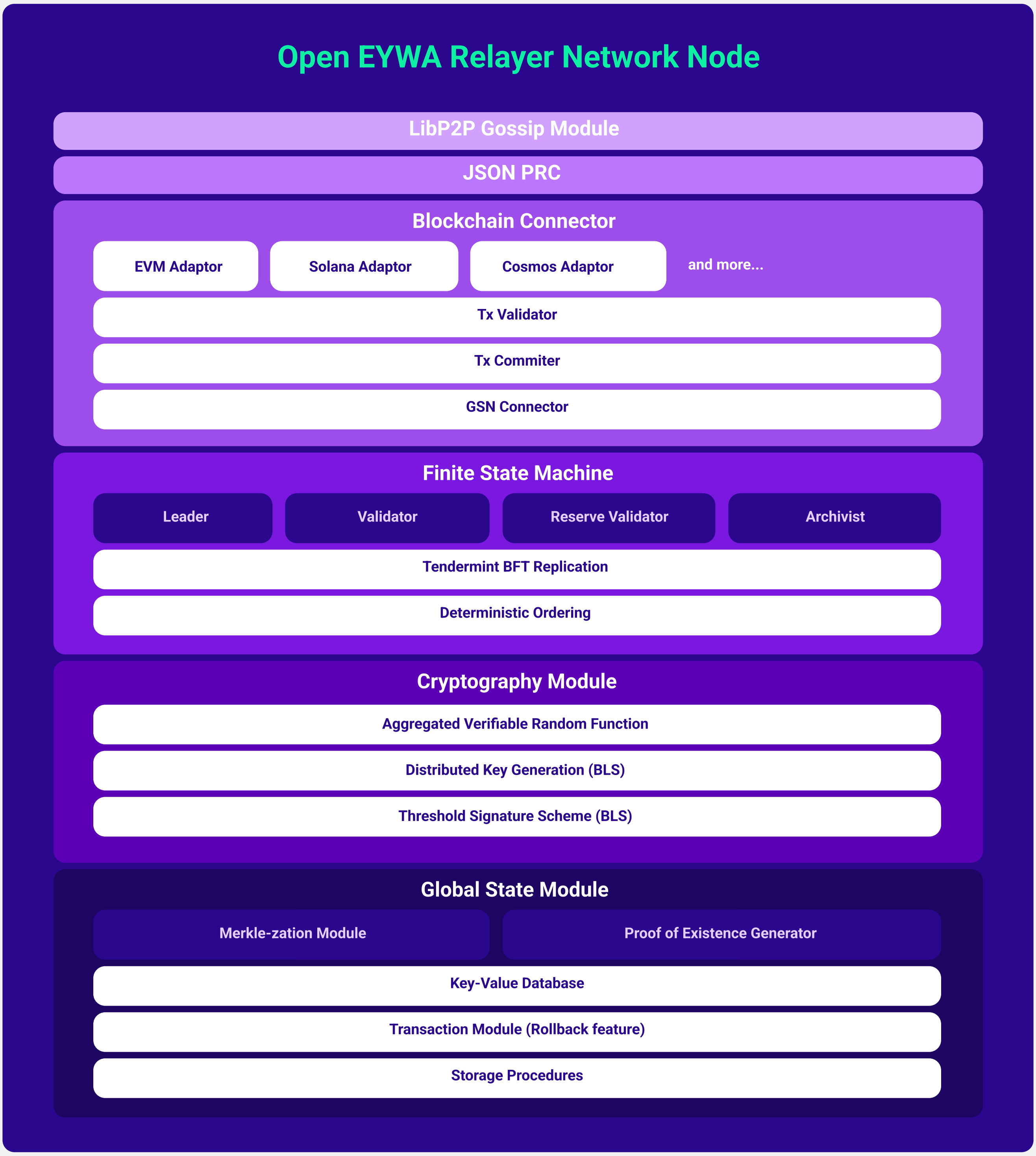
To implement the entire spectrum of interactions, the protocol uses only five types of requests:

1. From network A to network B
2. From Network A to the oracle network
3. From the oracle network to Network A
4. From the oracle network to all networks
5. From the oracle network to the oracle Network

The epoch change algorithm is similar to the processing of a cross-chain call, but it requires checking whether the participants correspond to the state in the protocol governance network, and not whether there is an initial call for action. During the normal operation of the protocol, the leader, validators and archivist are engaged in forming a request for changing the epoch, validation and execution, but to eliminate the possibility of blocking the epoch change by validators, the role of backup validators is necessary, whose job is to force the epoch change.

EYWA Oracle Network Node Architecture

The protocol network is a peer-to-peer network of oracles - EYWA Oracle Network. The oracle software has a modular architecture, the modules of which can optionally be disabled depending on the purpose of the node.



LibP2P Gossip - organization of the p2p network and messaging over the Internet.
JSON RPC - external API.
Blockchain Connector - interaction with blockchain networks.
FSM - organization of scenarios and rules of operation.
Cryptography - implementation of cryptographic methods
Global State - storage and management of the network state: balances, collateral, rewards, etc.

LibP2P Gossip

Effective messages exchange system is critical for building a large peer-to-peer network. The EYWA Oracle Network peer-to-peer network is based on the open libP2P library used in IPFS, Substrate projects. Out of the box, the library allows us to build distributed hash tables for searching for nearest neighbors and organize a gossip protocol with cryptographic proofs of message consistency.

JSON RPC

A method of remote interaction with a node that is familiar for a centralized infrastructure. Allows us to conveniently implement the ability to call remote procedures and receive data.

External programming interface is required for:

- Managing your own node
- **Receiving data:**
  Proof of inclusion;
  Network states: balances, collateral, epoch, etc.
  Information about processed and pending requests.
- Sending requests without a source network (from the oracle network to the recipient network).

Blockchain Connector

A module that unifies interactions with homogeneous networks. The need to support a large sample of networks requires separating business logic from the specifics of interaction with a specific network. For each network (or network type, for example, Ethereum-like), a unique adapter is created that allows:

- Check a request
- Verify a transaction
- Send a transaction
- (Optional) Send a transaction without funds to pay for network operation (GSN)

Deterministic Finite State Machine

Finite state machine (FSM) — is a method for describing rules and scenarios for executing business logic. For the operation of a decentralized protocol, a finite state machine is required to meet the following requirements:

- Deterministic execution of scripts regardless of the environment;
- Deterministic sorting of commands;
- Replication resistant to Byzantine behavior;

To fulfill all the requirements, EYWA Oracle Network uses the Termint solution, which shows excellent results within the Cosmos Hub.

Cryptography Module

The consensus of the protocol depends on the implementation of three cryptographic procedures:

- Distributed Key Generation;
- Threshold Signature Scheme;

- Verifiable Random Function;
- Global State Module.

The global state of the network is stored in the key-value database, without requirements for the structure of values and the type of keys.

To operate with the state in finite blockchain networks without the need to replicate the entire state, Merkle trees-based proofs are used. Merkle trees is a basic approach for proving honesty and including part of the data in the general data without the need to provide general data. Merkle's proofs are widely used in all decentralized networks, from simplified proof of payment in Bitcoin to proof of the Ethereum virtual machine state.

Potential attack vectors

Hindering the functioning of the protocol through non-fulfillment of the leader's obligations to form packets

Since the Internet does not guarantee the delivery of messages and the elected leader may experience connection problems without deliberately malicious intent, the penalty is the lack of a reward for the proposed packet. Therefore, the only way to compensate for the costs of the lottery to the participant who received the role of leader is to regularly form correct packets.

Hindering the functioning of the protocol through non-fulfillment of the archivist's obligations to publish and sign packets for the governance network

The user experience depends on the proper work of archivists, and therefore the protocol ensures punishment for their incorrect work. If the packet was formed and prepared for publication, but this action did not follow within the allotted period for this, then all requests and rewards are transferred to the next packet, and a special action is added that fines the archivist for the amount set by the protocol settings.

Generating packets with actions that do not pass verification

If validators received a packet from a leader containing actions that go against the general rules (unauthorized receipt of reward, requests without a source, or any other changes that do not pass verification), the leader is recognized as an attacker and is fined in the next packet for the amount set by the protocol. This fine must be reflected in the next packet, otherwise the subsequent leader will be recognized as an accomplice and will also be punished.

Hindering the functioning of the protocol through failure to fulfill the obligations of validators

The user experience depends on the proper work of the validators and the protocol introduces a number of penalties if a packet was offered, but no actions were taken within the allotted time for validation and signing of these actions.

Validation and signature depends on the stable operation of all validators to form a collective signature. Taking into account the problems described above, there is a possibility that most validators may not be physically able to form a signature without malicious intent

Therefore, if validators experienced temporary difficulties and were able to return to work before the end of the epoch, they lose only the reward for missed packets.

If the validators could not return to work before the end of the epoch, the epoch is changed at the initiative of the backup validators and the current circle of validators will be fined for the amount set by the protocol settings.

EYWA Cross-chain Bridge

To move value between blockchains, we use synthetic assets - EYWA tokens, or e-tokens. E-tokens are created whenever someone needs to move an asset between two blockchains.

Let's take a look at the example:

Bob moves x_A token from blockchain A to blockchain B. We use the following approach:

Bob sends a transaction to the EYWA Cross-chain Bridge, the original x_A token is blocked in the Portal smart contract in the A blockchain, this transaction triggers an event in the Bridge smart contract. This event is tracked and processed by oracles of EYWA Oracle Network.

They verify incoming transactions and make cross-chain calls of smart contracts in destination blockchains. In our example, Bob's transaction will trigger the Synthesis smart contract in blockchain B, which will issue a synthetic ex_A, token in blockchain B, backed by the x_A. token blocked in blockchain A.

At the same time, Bob can perform the reverse conversion at any time and take the original asset x_A.

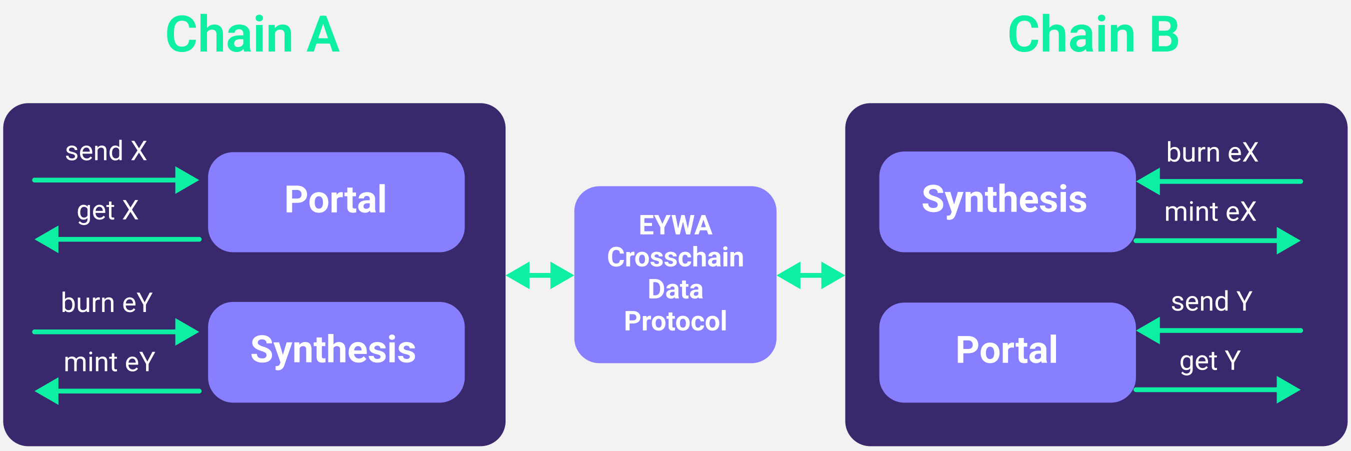
Thus, EYWA Cross-chain Bridge performs cross-chain transformations of the following form:
$s(x_A ,A ,B)=ex_A$- synthesis (mint) function for transfer from chain A to chain B

$u(ex_A ,B ,A)=x_A$ - unsynthesis (burn) function for transfer from chain B to chain A **$s(y_B,B,A)= ey_B$**

$u(ey_B,A ,B)= y_B$

$\forall x , ey , \in A\ \forall y , ex , \forall A,B \in S_{AB\ BA}$

Where A, B are blockchains from the S-set of blockchains with smart contracts. The EYWA Cross-chain Bridge consists of Portal and Synthesis smart contracts located in each of the blockchains A, B and uses EYWA Cross-chain Data Protocol (CDP) to transfer cross-chain calls between them.



EYWA Cross-chain Liquidity Protocol

The EYWA liquidity protocol includes smart contracts of EYWA Cross-chain Bridge deployed in a variety of blockchains and contracts of AMM exchanges deployed in each of the connected blockchains. This is necessary in order to provide liquidity for EYWA synthetic assets. Since users expect to receive a liquid asset when moving between blockchains, we ensure this by creating liquidity pools with synthetic assets.

For example: a user moves 100 USDT (erc20) from Ethereum to Binance Smart Chain and expects to receive 100 USDT (bep20), in order to ensure such an exchange, we will perform the following chain of actions:

- 100 USDT (erc20) is blocked in the Portal smart contract in Ethereum, an event is created in the Bridge contract, which EYWA Oracle Network nodes begin to process.
- EYWA Oracle Network calls the Bridge smart contract in Binance Smart Chain, sending information there to call the Synthesis smart contract.
- Synthesis executes a call and synthesizes 100 eUSDT(ETH) tokens and sends them to the user.
- 100 eUSDT(ETH) is exchanged for 100 USDT in the eUSDT(ETH)/ USDT liquidity pool (Uniswap v2 like pool), where USDT is a native bep20 token in Binance Smart Chain.

Exactly the same mechanism will allow you to exchange arbitrary assets from different blockchains. We intend to implement support for various AMM models that are most suitable for different types of assets: stable pools (Curve) for assets with the same price, classic Uniswap v2 pools for assets with different prices, Uniswap v3 pools with the ability to control the price range in which liquidity is provided and Balancer v2 for combining assets of different types into one pool.

A user can add or remove liquidity (create a pool of liquidity) in assets xA f rom blockchain A and yB from blockchain B and get his LP token in network A or B, to choose from. In this case, a liquidity pool is created in the target blockchain (for example, B) and the following transformations occur:

$s(x_A, A, B)=ex_A$- moving x_A from chain A to chain B,
$x\ ,\ ey \in A;\ y\ ,ex\ ,Lp \in B,\quad A,B \in S_{ABBAB}$

$ex_A+y_B=>Lp_B(ex_A, y_B)$ - adding liquidity in blockchain B,
$\forall x\ \ \exists ex => \exists Lp\ (ex\ ,\ y)\ \forall y\ ,ex_{AA\ BABBA}$

where **ex_A** - is a synthetic asset issued on blockchain B by locking the original asset x_A in the original blockchain A.

Lp_B - is a token of a cross-chain liquidity pool in blockchain B, consisting of a synthetic asset ex_A and a native one y_B.

When removing liquidity, the reverse process occurs with the possibility of obtaining liquidity either in the original assets and networks, or to obtain the original asset plus a synthetic asset.

$removeLp_B(ex_A, y_B) =>ex_A+y_B$ - removing liquidity from the pool in blockchain B,

$u(ex_A, B, A)=x_A$ -moving x_A from blockchain B back to A by burning ex_A.

Users can perform any exchange operations between native and / or synthetic assets within the pools available on each of the blockchains.

Legal information

PLEASE READ THIS SECTION AND THE FOLLOWING SECTIONS ENTITLED "DISCLAIMER OF LIABILITY", "NO REPRESENTATIONS AND WARRANTIES", "REPRESENTATIONS AND WARRANTIES BY YOU", "CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS", "MARKET AND INDUSTRY INFORMATION AND NO CONSENT OF OTHER PERSONS", "NO

ADVICE", "NO FURTHER INFORMATION OR UPDATE", "RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION", "NO OFFER OF SECURITIES OR REGISTRATION" AND "RISKS AND UNCERTAINTIES" CAREFULLY.

IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, PLEASE CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S).

EYWA Tokens are not intended to constitute securities in any jurisdiction. This White Paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction.

This White Paper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by the distributor/vendor of EYWA Tokens (the "Distributor") to purchase any EYWA Tokens, nor shall it or any part of it, nor the fact of its presentation form the basis of, or be relied upon in connection with any contract or investment decision.

The Distributor will be EYWA ("EYWA"), and will deploy all proceeds of sale of the EYWA Tokens to fund EYWA's cryptocurrency project, businesses and operations.

No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of the EYWA Tokens and no cryptocurrency or other form of payment is to be accepted on the basis of this White Paper.

Any agreement as between the Distributor and you as a purchaser, and in relation to any sale and purchase, of EYWA Tokens (as referred to in this White Paper) is to be governed by only a separate document setting out the terms and conditions (the "Terms and Conditions") of such an agreement. In the event of any inconsistencies between the Terms and Conditions and this White Paper, the former shall prevail.

You are not eligible and you are not to purchase any EYWA Tokens in the EYWA Initial Token Sale (as referred to in this White Paper) if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a citizen or resident of the Republic of Singapore.

No regulatory authority has examined or approved of any of the information set out in this White Paper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this White Paper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

There are risks and uncertainties associated with EYWA and/or the Distributor and their respective businesses and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in this White Paper).

This White Paper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of this White Paper is prohibited or restricted.

No part of this White Paper is to be reproduced, distributed or disseminated without including this section and the following sections entitled “Disclaimer of Liability”, “No Representations and Warranties”, “Representations and Warranties By You”, “Cautionary Note On Forward-Looking Statements”, “Market and Industry Information and No Consent of Other Persons”, “Terms Used”, “No Advice”, “No Further Information or Update”, “Restrictions On Distribution and Dissemination”, “No Offer of Securities Or Registration” and “Risks and Uncertainties”.

DISCLAIMER OF LIABILITY

To the maximum extent permitted by the applicable laws, regulations and rules, EYWA and/or the Distributor shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this White Paper or any part thereof by you.

NO REPRESENTATIONS AND WARRANTIES

EYWA and/or the Distributor does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this White Paper.

REPRESENTATIONS AND WARRANTIES BY YOU

By accessing and/or accepting possession of any information in this White Paper or such part thereof (as the case may be), you represent and warrant to EYWA and/or the Distributor as follows:

(a) you agree and acknowledge that the EYWA Tokens do not constitute securities in any form in any jurisdiction;

(b) you agree and acknowledge that this White Paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities in any jurisdiction or a solicitation for investment in securities and you are not bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this White Paper;

(c) you agree and acknowledge that no regulatory authority has examined or approved of the information set out in this White Paper, no action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction and the publication, distribution or dissemination of this White Paper to you does not imply that the applicable laws, regulatory requirements or rules have been complied with;

(d) you agree and acknowledge that this White Paper, the undertaking and/or the completion of the EYWA Initial Token Sale, or future trading of the EYWA Tokens on any cryptocurrency exchange, shall not be construed, interpreted or deemed by you as an indication of the merits of the EYWA and/or the Distributor, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in this White Paper);

(d) you agree and acknowledge that this White Paper, the undertaking and/or the completion of the EYWA Initial Token Sale, or future trading of the EYWA Tokens on any cryptocurrency exchange, shall not be construed, interpreted or deemed by you as an indication of the merits of the EYWA and/or the Distributor, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in this White Paper);

(e) the distribution or dissemination of this White Paper, any part thereof or any copy thereof, or acceptance of the same by you, is not prohibited or restricted by the applicable laws, regulations or rules in your jurisdiction, and where any restrictions in relation to possession are applicable, you have observed and complied with all such restrictions at your own expense and without liability to EYWA and/or the Distributor;

(f) you agree and acknowledge that in the case where you wish to purchase any EYWA Tokens, the EYWA Tokens are not to be construed, interpreted, classified or treated as:

(i) any kind of currency other than cryptocurrency;
(ii) debentures, stocks or shares issued by any person or entity (whether EYWA and/or the Distributor);
(i) rights, options or derivatives in respect of such debentures, stocks or shares;
(ii) rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;
(iii) units in a collective investment scheme;
(iv) units in a business trust;
(v) derivatives of units in a business trust; or
(vi) any other security or class of securities.

(g) you are fully aware of and understand that you are not eligible to purchase any EYWA Tokens if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a citizen or resident of the Republic of Singapore;

(h) you have a basic degree of understanding of the operation, functionality, usage, storage, transmission mechanisms and other material characteristics of cryptocurrencies, blockchain-based software systems, cryptocurrency wallets or other related token storage mechanisms, blockchain technology and smart contract technology;

(i) you are fully aware and understand that in the case where you wish to purchase any EYWA Tokens, there are risks associated with EYWA and the Distributor and their respective business and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper);

(j) you agree and acknowledge that neither EYWA nor the Distributor is liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this White Paper or any part thereof by you; and

(k) all of the above representations and warranties are true, complete, accurate and non-misleading from the time of your access to and/or acceptance of possession this White Paper or such part thereof (as the case may be).

CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS

All statements contained in this White Paper, statements made in press releases or in any place accessible by the public and oral statements that may be made by EYWA and/or the Distributor or their respective directors, executive officers or employees acting on behalf of EYWA or the Distributor (as the case may be), that are not statements of historical fact, constitute “forward- looking statements”. Some of these statements can be identified by forward-looking terms such as “aim”, “target”, “anticipate”, “believe”, “could”, “estimate”, “expect”, “if”, “intend”, “may”, “plan”, “possible”, “probable”, “project”, “should”, “would”, “will” or other similar terms. However, these terms are not the exclusive means of identifying forward-looking statements. All statements regarding EYWA’s and/or the Distributor’s financial position, business strategies, plans and prospects and the future prospects of the industry which EYWA and/or the Distributor is in are forward-looking statements. These forward-looking statements, including but not limited to statements as to EYWA’s and/or the Distributor’s revenue and profitability, prospects, future plans, other expected industry trends and other matters discussed in this White Paper regarding EYWA and/or the Distributor are matters that are not historic facts, but only predictions.

These forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results, performance or achievements of EYWA and/or the Distributor to be materially different from any future results, performance or achievements expected, expressed or implied by such forward-looking statements. These factors include, amongst others:

(a) changes in political, social, economic and stock or cryptocurrency market conditions, and the regulatory environment in the countries in which EYWA and/or the Distributor conducts its respective businesses and operations;

(b) the risk that EYWA and/or the Distributor may be unable or execute or implement their respective business strategies and future plans;

(c) changes in interest rates and exchange rates of fiat currencies and cryptocurrencies;

(d) changes in the anticipated growth strategies and expected internal growth of EYWA and/or the Distributor;

(e) changes in the availability and fees payable to EYWA and/or the Distributor in connection with their respective businesses and operations;

(f) changes in the availability and salaries of employees who are required by EYWA and/or the Distributor to operate their respective businesses and operations;

(g) changes in preferences of customers of EYWA and/or the Distributor;

(h) changes in competitive conditions under which EYWA and/or the Distributor operate, and the ability of EYWA and/or the Distributor to compete under such conditions;

(i) changes in the future liquidity needs of EYWA and/or the Distributor and the availability of liquidity to fund such needs;

(j) war or acts of international or domestic terrorism;

(k) occurrences of catastrophic events, natural disasters and acts of God that affect the businesses and/or operations of EYWA and/or the Distributor;

(l) other factors beyond the control of EYWA and/or the Distributor; and

(m) any risk and uncertainties associated with EYWA and/or the Distributor and their businesses and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper).

All forward-looking statements made by or attributable to EYWA and/or the Distributor or persons acting on behalf of EYWA and/or the Distributor are expressly qualified in their entirety by such factors. Given that risks and uncertainties that may cause the actual future results, performance or achievements of EYWA and/or the Distributor to be materially different from that expected, expressed or implied by the forward- looking statements in this White Paper, undue reliance must not be placed on these statements. These forward-looking statements are applicable only as of the date of this White Paper.

Neither EYWA, the Distributor nor any other person represents, warrants and/or undertakes that the actual future results, performance or achievements of EYWA and/or the Distributor will be as discussed in those forward-looking statements. The actual results, performance or achievements of EYWA and/or the Distributor may differ materially from those anticipated in these forward- looking statements.

Nothing contained in this White Paper is or may be relied upon as a promise, representation or undertaking as to the future performance or policies of EYWA and/or the Distributor.

Further, EYWA and/or the Distributor disclaim any responsibility to update any of those forward- looking statements or publicly announce any revisions to those forward-looking statements to reflect future developments, events or circumstances, even if new information becomes available or other events occur in the future.

MARKET AND INDUSTRY INFORMATION AND NO CONSENT OF OTHER PERSONS

This White Paper includes market and industry information and forecasts that have been obtained from internal surveys, reports and studies, where appropriate, as well as market research, publicly available information and industry publications. Such surveys, reports, studies, market research, publicly available information and publications generally state that the information that they contain has been obtained from sources believed to be reliable, but there can be no assurance as to the accuracy or completeness of such included information.

Save for EYWA, the Distributor and their respective directors, executive officers and employees, no person has provided his or her consent to the inclusion of his or her name and/or other information attributed or perceived to be attributed to such person in connection therewith in this White Paper and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information by such person and such persons shall not be obliged to provide any updates.

While EYWA and/or the Distributor have taken reasonable actions to ensure that the information is extracted accurately and in its proper context, EYWA and/or the Distributor have not conducted any independent review of the information extracted from third party sources, verified the accuracy or completeness of such information or ascertained the underlying economic assumptions relied upon therein. Consequently, neither EYWA, the Distributor, nor their respective directors, executive officers and employees acting on their behalf makes any representation or warranty as to the accuracy or completeness of such information and shall not be obliged to provide any updates on the same.

TERMS USED

To facilitate a better understanding of the EYWA Tokens being offered for purchase by the Distributor, and the businesses and operations of EYWA and/or the Distributor, certain technical terms and abbreviations, as well as, in certain instances, their descriptions, have been used in this White Paper. These descriptions and assigned meanings should not be treated as being definitive of their meanings and may not correspond to standard industry meanings or usage.

Words importing the singular shall, where applicable, include the plural and vice versa and words importing the masculine gender shall, where applicable, include the feminine and neuter genders and vice versa. References to persons shall include corporations.

NO ADVICE

No information in this White Paper should be considered to be business, legal, financial or tax advice regarding EYWA, the Distributor, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper). You should consult your own legal, financial, tax or other professional adviser regarding EYWA and/or the Distributor and their respective businesses and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper). You should be aware that you may be required to bear the financial risk of any purchase of EYWA Tokens for an indefinite period of time.

NO FURTHER INFORMATION OR UPDATE

No person has been or is authorised to give any information or representation not contained in this White Paper in connection with EYWA and/or the Distributor and their respective businesses and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper) and, if given, such information or representation must not be relied upon as having been authorised by or on behalf of EYWA and/or the Distributor. The EYWA Initial Token Sale (as referred to in the White Paper) shall not, under any circumstances, constitute a continuing representation or create any suggestion or implication that there has been no change, or development reasonably likely to involve a material change in the affairs, conditions and prospects of EYWA and/or the Distributor or in any statement of fact or information contained in this White Paper since the date hereof.

RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION

The distribution or dissemination of this White Paper or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of this White Paper or such part thereof (as the case may be) at your own expense and without liability to EYWA and/or the Distributor.

Persons to whom a copy of this White Paper has been distributed or disseminated, provided access to or who otherwise have the White Paper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this White Paper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

NO OFFER OF SECURITIES OR REGISTRATION

This White Paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. No person is bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this White Paper. Any agreement in relation to any sale and purchase of EYWA Tokens (as referred to in this White Paper) is to be governed by only the Terms and Conditions of such agreement and no other document. In the event of any inconsistencies between the Terms and Conditions and this White Paper, the former shall prevail.

You are not eligible to purchase any EYWA Tokens in the EYWA Initial Token Sale (as referred to in this White Paper) if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a citizen or resident of the Republic of Singapore.

No regulatory authority has examined or approved of any of the information set out in this White Paper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this White Paper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

RISKS AND UNCERTAINTIES

Prospective purchasers of EYWA Tokens (as referred to in this White Paper) should carefully consider and evaluate all risks and uncertainties associated with EYWA, the Distributor and their respective businesses and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper), all information set out in this White Paper and the Terms and Conditions prior to any purchase of EYWA Tokens. If any of such risks and uncertainties develops into actual events, the business, financial condition, results of operations and prospects of EYWA and/or the Distributor could be materially and adversely affected. In such cases, you may lose all or part of the value of the EYWA Tokens.

Source

1 Vitalik Buterin on sharding
https://vitalik.ca/general/2021/04/07/sharding.html

2 Binance cross-chain bridge
https://www.binance.org/en/bridge

3 ThorChain cross-chain liqidity network
https://www.thorchain.com/

4 Anyswap DEX
https://anyswap.net/

5 Axelar Network cross-chain interoperability protocol
https://axelar.network/

6 NEAR blockchain compatibility with Ethereum
https://near.org/blog/eth-near-rainbow-bridge

7 Threshold cryptosystem basics
https://en.wikipedia.org/wiki/Threshold_cryptosystem

8 Whitepaper PolyNework
https://www.poly.network/PolyNetwork-whitepaper.pdf

9 REN Project cross-chain liquidity transfer protocol
https://renproject.io/

10 REN Project second website
https://www.darknodes.io/

11 REN Project Github
https://github.com/renproject/ren/wiki/Phases

12 REN Project release
https://medium.com/renproject/going-live-with-renvm-v0-4-941fb097e983

13 PolyNework Whitepaper
https://www.poly.network/PolyNetwork-whitepaper.pdf

14 PolyNetwork Hacked
https://medium.com/poly-network/honour-exploit-and-code-how-we-lost- 610m-dollar-and-got-it-back-c4a7d0606267

15 Cosmos Stargate IBC
https://stargate.cosmos.network/

16 Fusion Yellowpaper
https://www.fusion.org/themes/fusion/assets/pdf/Fusion-Yellow-Paper.pdf

17 FAQ Anyswap DEX
https://anyswap-faq.readthedocs.io/en/latest/index.html

18 Github Anyswap DEX
https://fusiondev.gitbook.io/fusion/dapps/anyswap|

19 Anyswap hacked
https://anyswap.medium.com/anyswap-multichain-router-v3-exploit-statement-6833f1b7e6fb

20 Antonell Multibridge Github
https://github.com/antonnell/multibridge.xyz

21 Anyswap cross-chain bridge
https://multichain.xyz/

22 Chainswap application for cross-chain transactions
https://chainswap.com/

23 Chainswap hacked
https://chain-swap.medium.com/asap-token-important-update-67073aae925c

24 ThorChain cross-chain liqidity network
https://thorchain.org/

25 ThorChain hack
https://medium.com/breadcrumbsapp/thorchain-heist-an-analysis-of-the-fund-flow-7ca18a18d044

26 ThorChain hack 2
https://medium.com/breadcrumbsapp/thorchain-hack-2-analysis-of-the-fund-flow-bb53f07b0f46

27 Whitepaper Polygon
https://polygon.technology/lightpaper-polygon.pdf

28 DFYN DEX Litepaper
https://www.dfyn.network/assets/docs/Dfyn-Litepaper.pdf

29 Binance cross-chain bridge
https://academy.binance.com/en/articles/an-introduction-to-binance- bridge

30 Chainlink cross-chain interoperability protocol
https://chain.link/solutions/cross-chain

31 Connext cross-chain interoperability protocol
https://docs.connext.network/

32 ChainBridge cross-chain interoperability protocol
https://chainbridge.chainsafe.io/

33 PR article about ChainBridge
https://medium.com/chainsafe-systems/a-bridge-to-a-new-world- 7627472eaf9d

34 Curve DEX
https://curve.fi/

35 Uniswap DEX
https://uniswap.org/

36 Balancer DEX
https://balancer.fi/

37 Horizen cross-chain platform
https://www.horizen.io/

38 Ethereum Gas Station Network project
https://opengsn.org/

39 Gnosis Safe crypto asset management platform
https://docs.gnosis.io/safe/

40 Ethereum EIP-712 signature standard
https://eips.ethereum.org/EIPS/eip-712#simple-summary

41 DAO basics
https://coinmarketcap.com/alexandria/article/what-is-a-dao

42 DAO basics
https://medium.com/smartz-blog/what-is-dao-and-how-it-works-d43ec5bc236f

43 Tendermint BFT engine
https://tendermint.com/core

44 BLS digital signature basics
https://en.wikipedia.org/wiki/BLS_digital_signature

45 Prisoner's dilemma basics
https://en.wikipedia.org/wiki/Prisoner%27s_dilemma

46 IoTeX Whitepaper
http://files.iotex.io/publications/IoTeX_Whitepaper_1.5_EN.pdf

47 Algorand Whitepaper
https://algorandcom.cdn.prismic.io/algorandcom%2Fa26acb80-b80c-46ff-a1ab-a8121f74f3a3_p51-gilad.pdf