

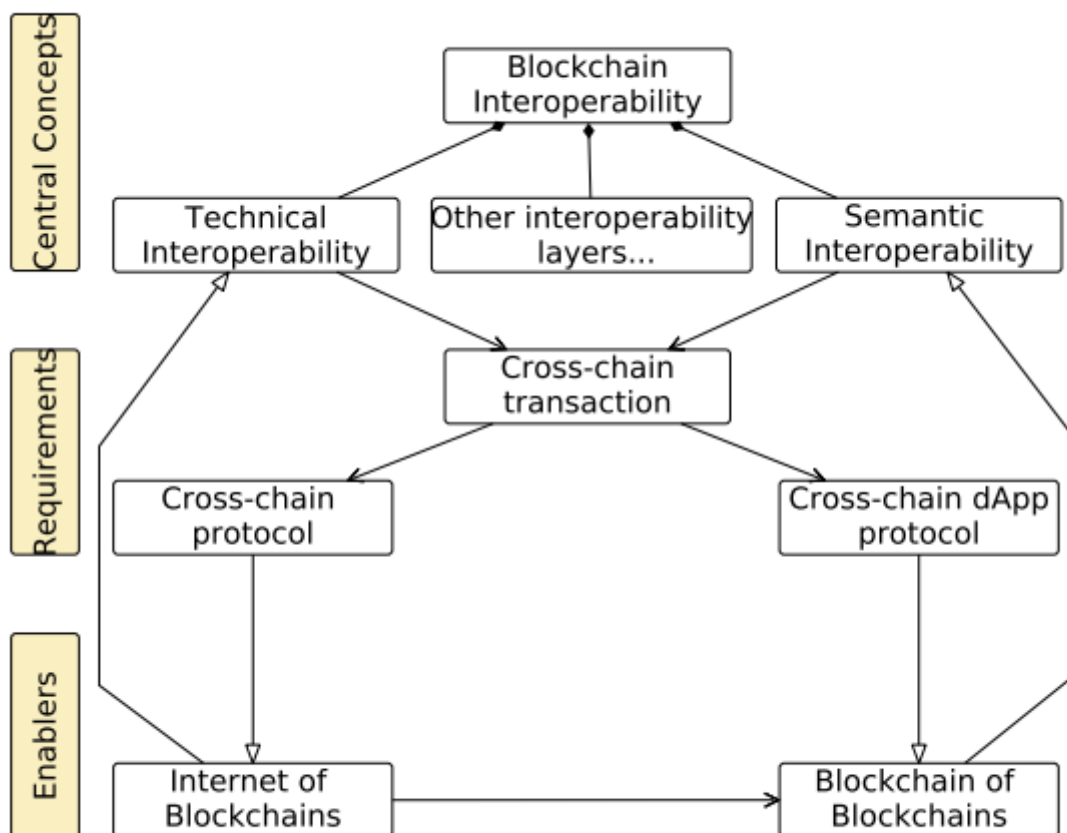
Interoperability

Introduction

See A Survey on Blockchain Interoperability (<https://arxiv.org/abs/2005.14282>) an SoK on blockchain interoperability

Developers have to choose between novelty and stability, leading to a vast diversity of choices.

This diversity leads to fragmentation : there are many immature blockchain solutions



Interoperability does not only conflate flexibility and application portability. It also has the potential to solve some of the biggest blockchain research challenges. In particular, interoperability promotes blockchain scalability, as it provides a way to offload transactions to other blockchains, e.g., via sharding, it can promote privacy

Cross-chain communication protocol (CCCP).

A CCCP allows homogeneous blockchains to communicate (sidechains typically do this)
For example transferring an asset in this way would typically involve 3 stages

1. locking (or extinguishing) of an asset on a source blockchain;
2. blockchain transfer commitment, and
3. creation of a representation of the asset on a target blockchain

Cross-blockchain communication protocol (CBCP)

CBCPs allow heterogeneous blockchains to communicate (e.g., the Interledger Protocol)

“The differentiation between CCCPs and CBCPs is important because CCCPs typically can leverage the interoperating blockchains’ constructs and functionality (e.g., utilize smart contracts to implement a relay), whereas CBCPs normally require blockchains to be adapted. However, CBCPs may leverage specific functionalities of both blockchains”

“There exists no cross-chain communication protocol tolerant against misbehaving nodes without a trusted third party”

Approaches

1. Sidechains

Here one blockchain (main chain) considers another blockchain as an extension of itself (the sidechain). The mainchain maintains a ledger of assets and is connected to the sidechain, a separate system attached to the main chain via a cross-chain communication protocol. An example is a two-way peg, a mechanism for transferring assets between the main chain and the sidechain.

A second layer can allow off-chain transactions between users through the exchange of messages tethered to a sidechain. A sidechain is then a construct that allows for offloading transactions from the mainchain, processes it, and can redirect the outcome of such processing back to the main chain.

2. Notary Schemes

A notary scheme involves a notary that is an entity that monitors multiple chains, triggering transactions in a chain upon an event (e.g., a smart contract is deployed) taking place on another chain. Notary schemes are, in practice, instantiated as centralized exchanges (EXs) or decentralized exchanges (DEXs)

0x implements a decentralized exchange as a set of smart contracts (called automated market makers), replacing an on-chain order book with a real-time price-adjustment model. 0x uses a hybrid implementation, “off-chain order relay with on-chain settlement”, combining the idea of a state channel with settlement smart contracts. Two parties participate: makers and takers. Makers place orders on the exchange, providing liquidity for the network (a set of decentralized exchanges), while takers place orders matched with the makers’ orders.

3. HTLC

Hashed time-locks contracts (HTLCs) initially appeared as an alternative to centralized exchanges, as they enable cross-chain atomic operations . HTLCs techniques use

hashlocks and timelocks to enforce atomicity of operations, normally between two parties.

4. Blockchain of Blockchains

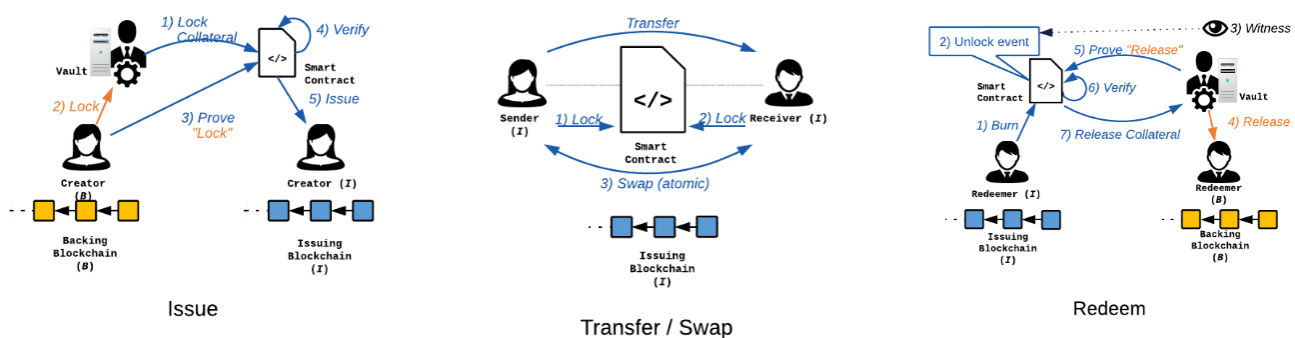
Blockchain of Blockchains are frameworks that provide reusable data, network, consensus, incentive, and contract layers for the creation of application-specific blockchains (customized blockchains) that interoperate between each other. For example Polkadot and Cosmos, both utilize the inter blockchain communication protocol (IBC)

5. Hybrid Connectors

Hybrid Connectors attempt at delivering a “blockchain abstraction layer”, capable of exposing a set of uniform operations allowing a dApp to interact with blockchains without the need of using different APIs

XClaim

Focussed on implementing Bitcoin-backed tokens on Ethereum,



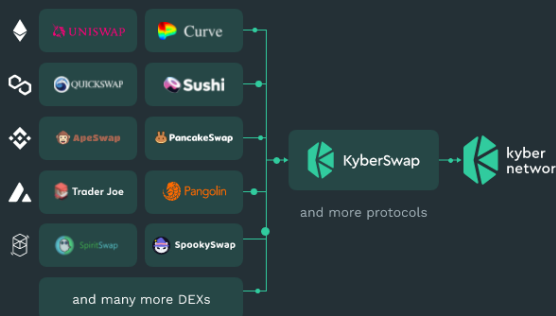
Features

- Secure audit logs: Logs are constructed to record actions of all users both on Bitcoin and Ethereum.
- Transaction inclusion proofs: Chain relays are used to prove correct behavior on Bitcoin to the smart contract on Ethereum.
- Proof-or-Punishment: Instead of relying on timely fraud proofs (reactive), XCLAIM requires correct behavior to be proven proactively.
- Over-collateralization: Non-trusted intermediaries are bound by collateral, with mechanisms in place to mitigate exchange rate fluctuations.

Other Bridges

Rainbow bridge (Near <> ETH)
tBTC (BTC <> ETH)

Kyber



HOW KYBER WORKS


Connecting Liquidity for Traders, Dapps and Aggregators

Kyber's technology connects the deepest crypto liquidity from diverse sources to provide the best rates and maximize returns for everyone. Swap tokens, earn yield, and build the best DeFi applications with Kyber.

\$25B+ TVL from DEXs	33+ DEXs	5+ Chains	20,000 Tokens
--------------------------------	--------------------	---------------------	-------------------------

Interledger

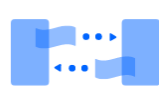
The Interledger Foundation is a non-profit advocate for the web, promoting innovation, creativity, and inclusion by advancing open payment standards and technologies that seamlessly connect our global society.




Interledger
FOUNDATION

[About Us](#) [Our Work](#) [Take Action](#) [FAQ](#) [Developer Tools](#) [NEWS](#) [Join](#)


We Believe




Monetary interaction should be as easy as information exchange.



Humans should be able to transfer their money with each other without any barriers or friction.



The unbanked and underbanked should have equitable access.



Content creators and digital innovators should be fairly compensated.

All of the work we do is to connect and benefit each and every human, regardless of identity, geography, or income.

In short, we believe connecting all currencies is connecting all of humanity.

Interledger is not tied to a single company, blockchain, or currency.



Code with Money

Add payments without being tied to a single currency or payment provider.



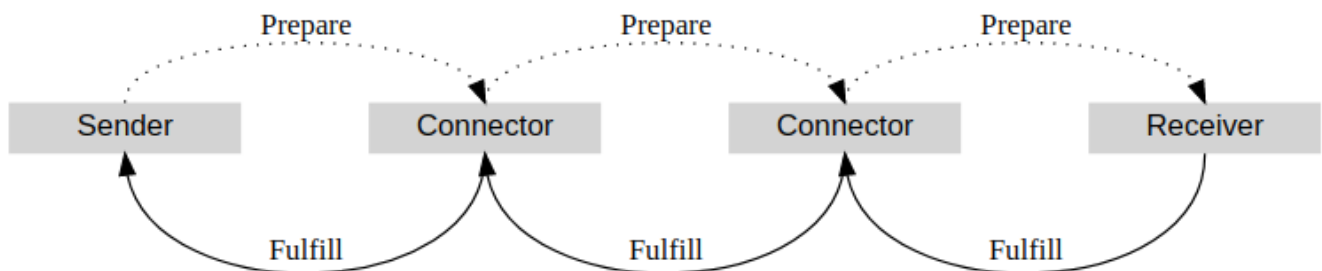
Multi-Hop Routing

Send payments to other ledgers, even if they are multiple hops away.

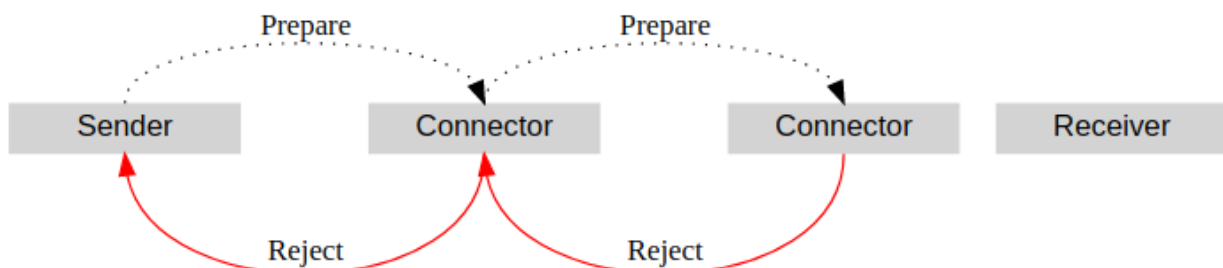


Simple Protocol

Inspired by TCP/IP, Interledger is easy to implement and use.



At any step along the way, a connector or the receiver can reject the payment, sending a "reject" packet back up the chain. This can happen if the receiver doesn't want the money, or a connector can't forward it. A prepared payment can also expire without the condition being fulfilled. In all these cases, no balances change.



Cosmos

Whitepaper (<https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md>)

Cosmos is a heterogeneous network of many independent parallel blockchains, each powered by classical BFT consensus algorithms like Tendermint

Serving as the economic center of Cosmos, the Cosmos Hub is a blockchain that provides vital services to the Interchain.



Marketplace

Set to operate a next-gen decentralized exchange, swapping digital assets from across the Interchain, with very low fees and instant transaction confirmation.



Security provider

With the upcoming Interchain Security feature, ATOM will soon be securing many chains, in exchange for additional staking rewards.



Router

A core mission of the Hub – to connect chains by establishing IBC connections with compatible chains and operating decentralized bridges with chains like Ethereum and Bitcoin.



Custodian

Located at the crossroads of the Interchain, the Hub is extremely secure, the best place to hold digital assets and manage accounts across many chains.

Capital Formation · Live



Staking →

Built on top of the **Tendermint BFT consensus engine**, the Hub's staking module is one of the most efficient proof-of-stake implementations in the world. It enables ATOM token holders to secure the chain by locking their ATOM, in exchange for transaction fees.

Governance · Live



Voting →



Staking ATOM gives rights to participate in the open governance process, which governs the evolution of the network.

Account System · 2021

Interchain Accounts



Interchain Accounts are the accounts of the IBC-enabled world. Essentially, they allow blockchains to securely control accounts on other chains over IBC. With this feature, users will be able to access the entire Interchain through their single Cosmos Hub account. One account, for all the chains.



  Chainapsis, Interchain GmbH

Capital Formation · Q2 2021



Gravity DEX →

The Cosmos Hub's Gravity DEX will enable users to seamlessly swap digital assets coming from all over the interchain. This service improves on existing designs by combining AMM features (like that of Uniswap) with an orderbook-based model, providing a richer and more efficient trading experience.

  B-Harvest, Tendermint

Gravity Bridge ↗

Backed by billions of dollars of ATOM staked on the Cosmos Hub, the Gravity Bridge will be the most secure, efficient, and decentralized cross chain bridge to Ethereum. It will enable Cosmos assets to flow into the Ethereum ecosystem as ERC-20 tokens and, conversely, native ERC-20 tokens to flow in the Cosmos ecosystem.

 Althea, Interchain Foundation

Shared Security · Late 2021

Interchain Security ↗

Staked ATOM will be able to secure more than just the Cosmos Hub. In practice, validators will be able to validate chains that request it (called child-chains) on an opt-in basis, with their ATOM delegation as collateral. In exchange for securing child-chains, ATOM stakers will be rewarded with additional rewards. The more child-chains, the more rewards!

 Informal Systems, Interchain Foundation, Tendermint

Service Discovery · 2021

Chain Name Service ↗


Just like websites have domain names, blockchains will have chain names. These chain names will be managed on the Cosmos Hub, which will operate a Chain Name Service. They will make it much easier for users of the Interchain to identify the chain(s) they want to interact with.

 Tendermint, Interchain Foundation

Capital Formation · 2022

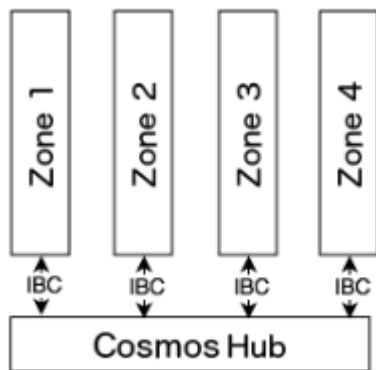
Liquid Staking ↗

Liquid Staking will be an important primitive in the cross-chain Defi space. At their core, liquid staking are claims against staked ATOM. Just like staked ATOM, liquid staking accrues staking rewards - but unlike staked ATOM, this type of staking is liquid, meaning the ATOM can be transferred. Since they represent staked ATOM, liquid staking are at risk of being partially burnt if the underlying ATOM get slashed.

 Chorus One, Interchain Foundation

Zones (sometimes called shards) are application specific blockchains built on the Cosmos SDK.

The first zone on Cosmos is called the Cosmos Hub.



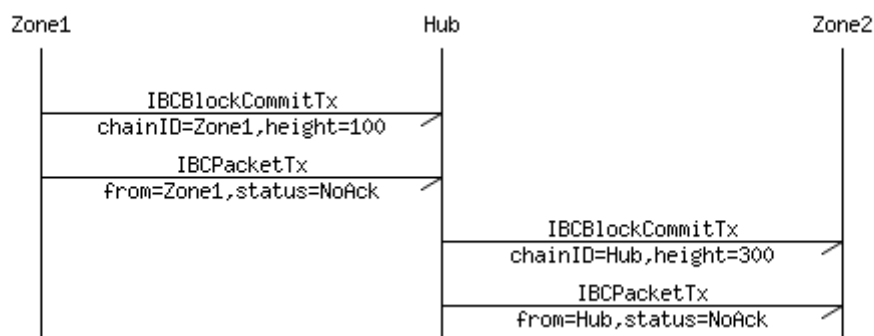
A constant stream of recent block commits from zones posted on the Hub allows the Hub to keep up with the state of each zone. Likewise, each zone keeps up with the state of the Hub (but zones do not keep up with each other except indirectly through the Hub). Packets of information are then communicated from one zone to another by posting Merkle-proofs as evidence that the information was sent and received. This mechanism is called inter-blockchain communication.

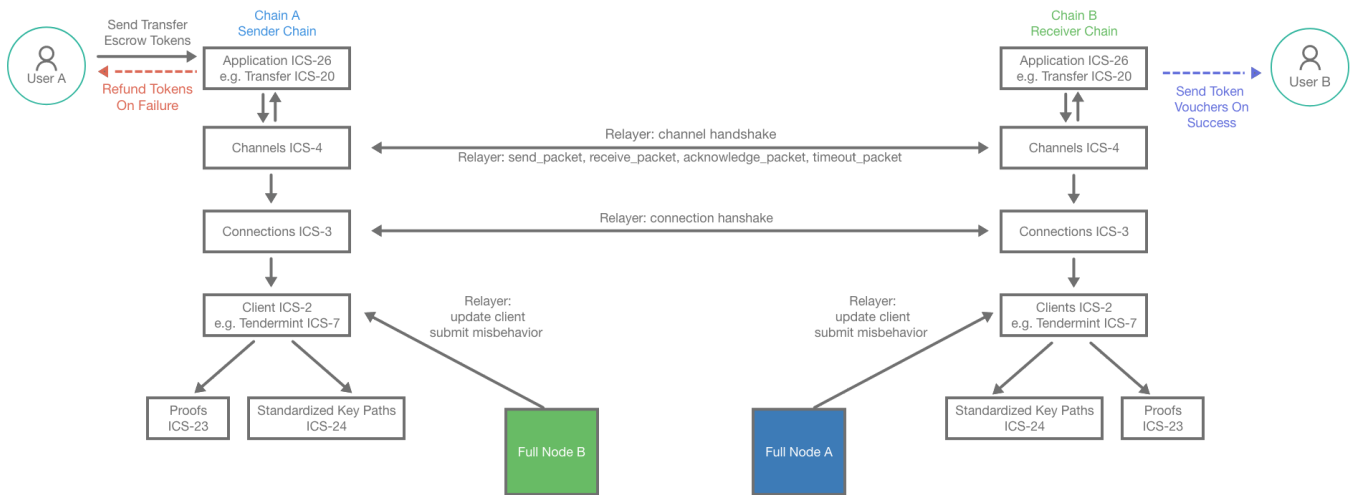
Inter-blockchain communication

See IBCProtocol (<https://ibcprotocol.org/>)

IBC resembles the Internet network layer as it routes arbitrary data packets to a target blockchain. A target blockchain can know that a certain ordered packet with arbitrary data came from another blockchain. By handling transportation and order, the protocol has several steps to achieve cross-zone transactions.

To move a packet from one blockchain to another, a proof is posted on the receiving chain. The proof states that the sending chain published a packet for the alleged destination. For the receiving chain to check this proof, it must be able keep up with the sender's block headers. This mechanism is similar to that used by sidechains, which requires two interacting chains to be aware of one another via a bidirectional stream of proof-of-existence datagrams (transactions).





IBC Components

1. Clients - IBC clients are light clients that are identified by a unique client id. IBC clients track the consensus states of other blockchains and the proof specs of those blockchains that are required to properly verify proofs against the client's consensus state.
2. Connections - Connections encapsulate two ConnectionEnd objects on two separate blockchains. Each ConnectionEnd is associated with a client of the other blockchain (the counterparty blockchain).
3. Proofs and paths In IBC, blockchains do not directly pass messages to each other over the network. To communicate, a blockchain commits some state to a precisely defined path reserved for a specific message type and a specific counterparty. A relayer process monitors for updates to these paths and relays messages by submitting the data stored under the path along with a proof of that data to the counterparty chain.

The Cosmos Hub is a multi-asset proof-of-stake cryptocurrency with a simple governance mechanism which enables the network to adapt and upgrade. In addition, the Cosmos Hub can be extended by connecting other zones.

Peg Zones (bridges) allow connection to specific blockchains such as Ethereum.

Polkadot



True interoperability

Polkadot enables cross-blockchain transfers of any type of data or asset, not just tokens. Connecting to Polkadot gives you the ability to interoperate with a wide variety of blockchains in the Polkadot network.



Economic & transactional scalability

Polkadot provides unprecedented economic scalability by enabling a common set of validators to secure multiple blockchains. Polkadot provides transactional scalability by spreading transactions across multiple parallel blockchains.



Easy blockchain innovation

Create a custom blockchain in minutes using the [Substrate](#) framework. Connect your chain to Polkadot and get interoperability and security from day one. This ease of development helps Polkadot's network grow.



Forkless and future-proof

Polkadot can upgrade without hard forks to integrate new features or fix bugs. This capability enables Polkadot to easily adapt to changes and upgrade itself as better technologies become available.



Security for everyone

Polkadot's novel data availability and validity scheme allows chains to interact with each other in a meaningful way. Chains remain independent in their governance, but united in their security.



User-driven network governance

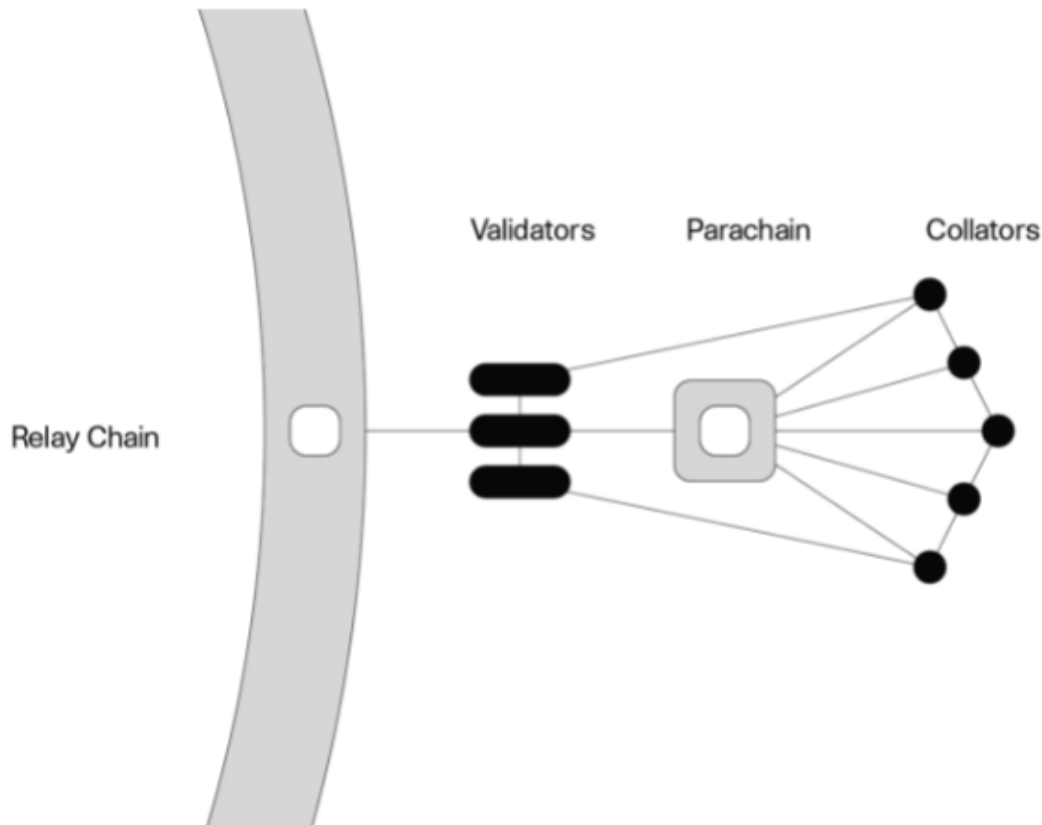
Polkadot has a sophisticated governance system where all stakeholders have a voice. Upgrades to the network are coordinated on-chain and enacted autonomously, ensuring that Polkadot's development reflects the values of the community and avoids stagnation.

See Wiki (<https://wiki.polkadot.network/docs/getting-started>)

“Polkadot is built to connect and secure unique blockchains, whether they be public, permission-less networks, private consortium chains, or oracles and other Web3 technologies. It enables an internet where independent blockchains can exchange information under common security guarantees.”

Parachain

A parachain is an application-specific data structure that is globally coherent and validatable by the validators of the Relay Chain.



They communicate with other parachains via XCM

Consensus - Nominated Proof of Stake

It is designed with the roles of validators and nominators, to maximize chain security. Actors who are interested in maintaining the network can run a validator node.

Validators assume the role of producing new blocks in BABE, validating parachain blocks, and guaranteeing finality. Nominators can choose to back select validators with their stake. Nominators can approve candidates that they trust and back them with their tokens.

Hybrid Consensus

Two protocols are used : GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement) and BABE (Blind Assignment for Blockchain Extension).

Hybrid consensus splits up the finality gadget from the block production mechanism.

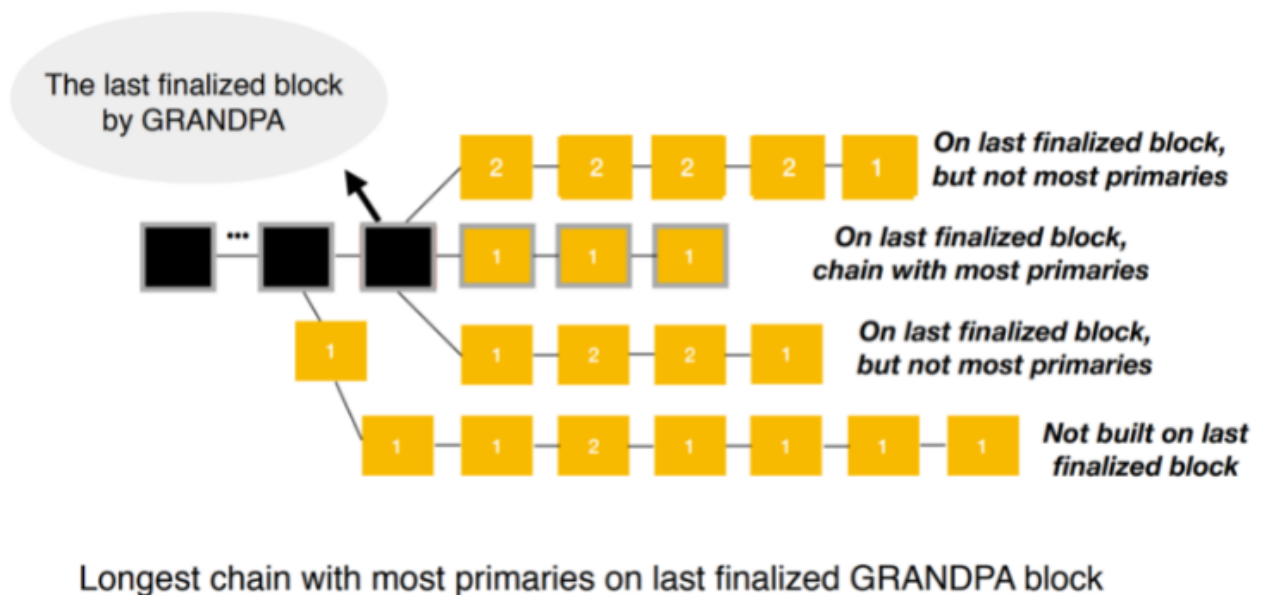
- BABE (Blind Assignment for Blockchain Extension) is the block production mechanism that runs between the validator nodes and determines the authors of new blocks. BABE assigns block production slots to validators according to stake and using the Polkadot randomness cycle.

- GRANDPA

It works in a partially synchronous network model as long as 2/3 of nodes are honest and can cope with 1/5 Byzantine nodes in an asynchronous setting. A notable distinction is that GRANDPA reaches agreements on chains rather than blocks, greatly speeding up the finalization process, even after long-term network partitioning or other networking failures. In other words, as soon as more than 2/3 of validators attest to a chain containing a certain block, all blocks leading up to that one are finalized at once.

Primary and Secondary Blocks

When no validators have rolled low enough in the randomness lottery to qualify for block production, a slot can remain seemingly blockless. We avoid this by running a secondary, round-robin style validator selection algorithm in the background. The validators selected to produce blocks through this algorithm always produce blocks, but these secondary blocks are ignored if the same slot also produces a primary block from a VRF-selected validator. Thus, a slot can have either a primary or a secondary block, and no slots are ever skipped.



Validators

Validators perform two functions:

1. Verifying that the information contained in an assigned set of parachain blocks is valid (such as the identities of the transacting parties and the subject matter of the contract).
2. Participating in the consensus mechanism to produce the Relay Chain blocks based on validity statements from other validators. Any instances of non-compliance with the consensus algorithms result in punishment by removal of some or all of the validator's staked DOT, thereby discouraging bad actors. Good performance, however, will be rewarded, with validators receiving block rewards (including transaction fees) in the form of DOT in exchange for their activities.

Collators

Collators maintain parachains by collecting parachain transactions from users and producing state transition proofs for Relay Chain validators. In other words, collators maintain parachains by aggregating parachain transactions into parachain block candidates and producing state transition proofs for validators based on those blocks.

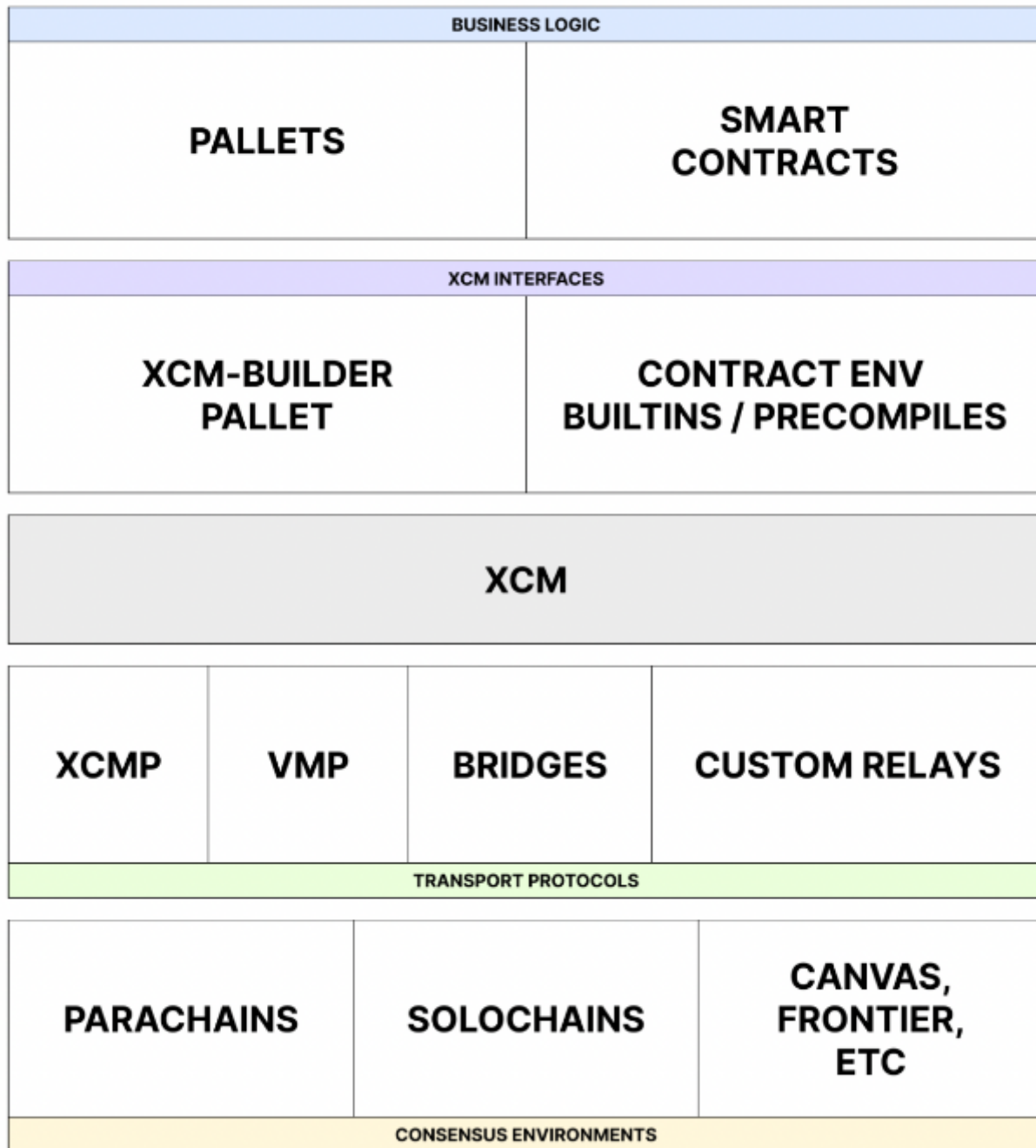
Upgrades

The network has an advanced suite of governance tools and, using the WebAssembly standard as a “meta-protocol”, can autonomously deploy network upgrades.

Cross-Consensus Message Format (XCM)

XCM cannot actually send messages between systems. It is a format for how message transfer should be performed, similar to how RESTful services use REST as an architectural style of deployment.

XCM Tech Stack



Vertical Message passing

- UMP (Upward Message Passing): allows parachains to send messages to their relay chain.
- DMP (Downward Message Passing): allows the relay chain to pass messages down to one of their parachains.

XCMP - Cross-Chain Message Passing (Still being developed)

It is the task of the Relay Chain validators to move transactions on the output queue of one parachain into the input queue of the destination parachain.

However, only the associated metadata is stored as a hash in the Relay Chain storage.

Example

A smart contract that exists on parachain A will route a message to parachain B in which another smart contract is called that makes a transfer of some assets within that chain.

Charlie executes the smart contract on parachain A, which initiates a new cross-chain message for the destination of a smart contract on parachain B.

The collator node of parachain A will place this new cross-chain message into its outbound messages queue, along with a destination and a timestamp.

The collator node of parachain B routinely pings all other collator nodes asking for new messages (filtering by the destination field). When the collator of parachain B makes its next ping, it will see this new message on parachain A and add it into its own inbound queue for processing into the next block.

Validators for parachain A will also read the outbound queue and know the message.

Validators for parachain B will do the same. This is so that they will be able to verify the message transmission happened.

Common Good Parachains

“Common Good” parachains are parachain slots reserved for functionality that benefits the ecosystem as a whole.

For example Statement for management of fungible and non fungible assets

Bridges

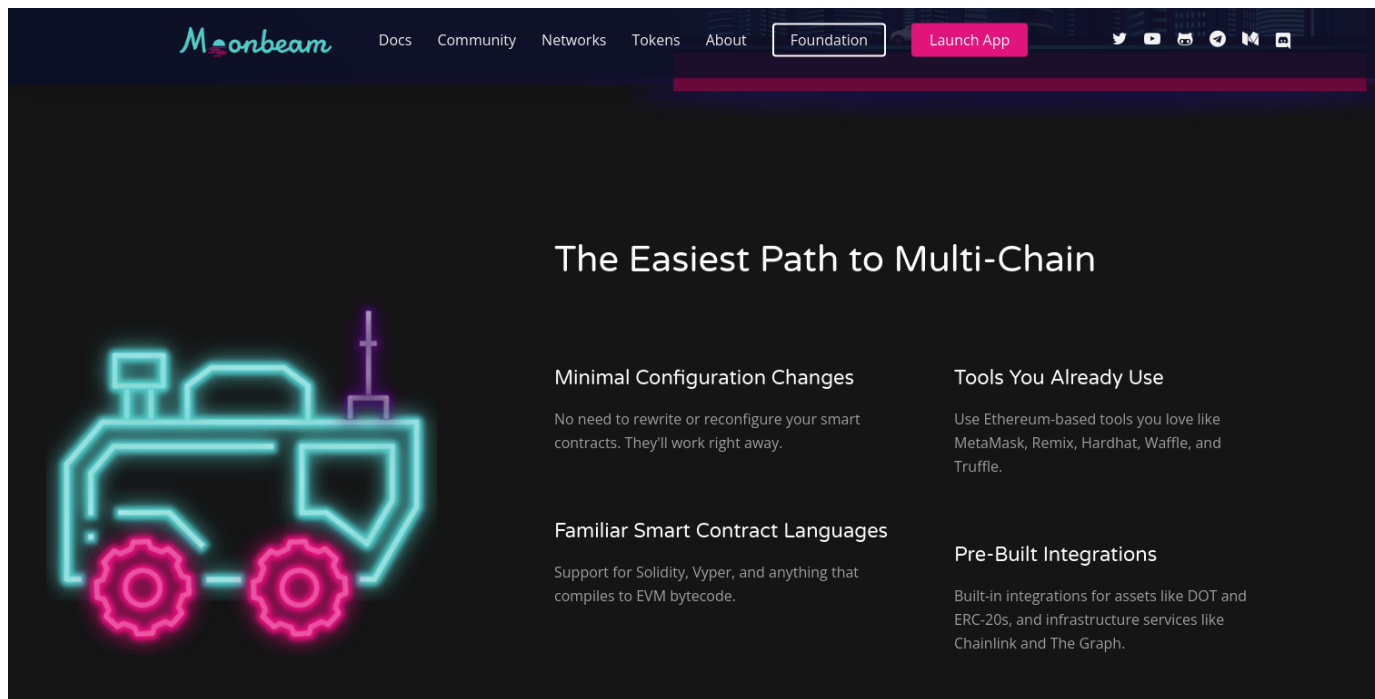
Types of bridge

- Bridge pallets - For Substrate-native chains, use a bridge pallet (e.g. Kusama <> Polkadot bridge, since both networks' parachains use Substrate).
- Smart contracts - If the chain is not on Substrate, you should have smart contracts on the non-Substrate chain to bridge (e.g. Ethereum mainnet will have a bridge smart contract that initiates Eth transactions based on incoming XCMP messages).
- Higher-order protocols - If your chain does not support smart contracts (e.g. Bitcoin), you should use XClaim or similar protocols to bridge.

Notable Parachains

Kusama

Kusama is a scalable network of specialized blockchains built using Substrate and nearly the same codebase as Polkadot. The network is an experimental development environment for teams who want to move fast and innovate on Kusama, or prepare for deployment on Polkadot.



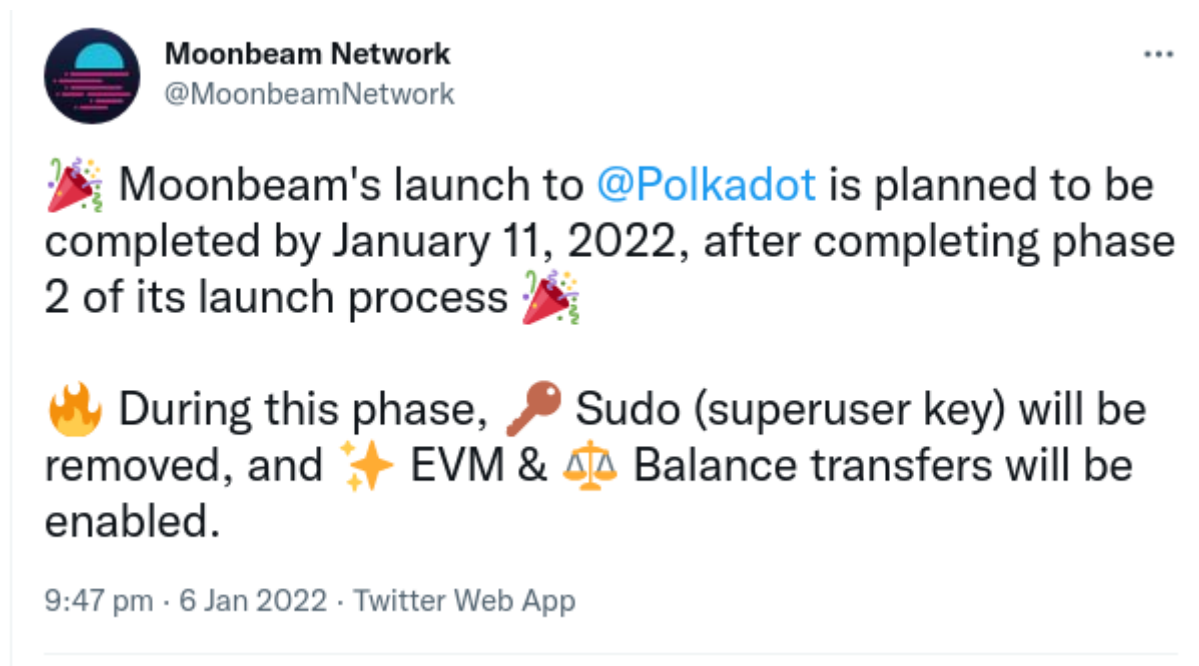
The Easiest Path to Multi-Chain

Minimal Configuration Changes
No need to rewrite or reconfigure your smart contracts. They'll work right away.

Familiar Smart Contract Languages
Support for Solidity, Vyper, and anything that compiles to EVM bytecode.

Tools You Already Use
Use Ethereum-based tools you love like MetaMask, Remix, Hardhat, Waffle, and Truffle.

Pre-Built Integrations
Built-in integrations for assets like DOT and ERC-20s, and infrastructure services like Chainlink and The Graph.



Moonbeam Network
@MoonbeamNetwork

🎉 Moonbeam's launch to @Polkadot is planned to be completed by January 11, 2022, after completing phase 2 of its launch process 🎉

🔥 During this phase, 🔑 Sudo (superuser key) will be removed, and ✨ EVM & ⚖️ Balance transfers will be enabled.

9:47 pm · 6 Jan 2022 · Twitter Web App

Comparison of Cosmos / Pokadot

See Comparison article (<https://wiki.polkadot.network/docs/learn-comparisons-cosmos>)

Scalability

Cosmos - manages about 1K tps, the bottleneck is consensus.

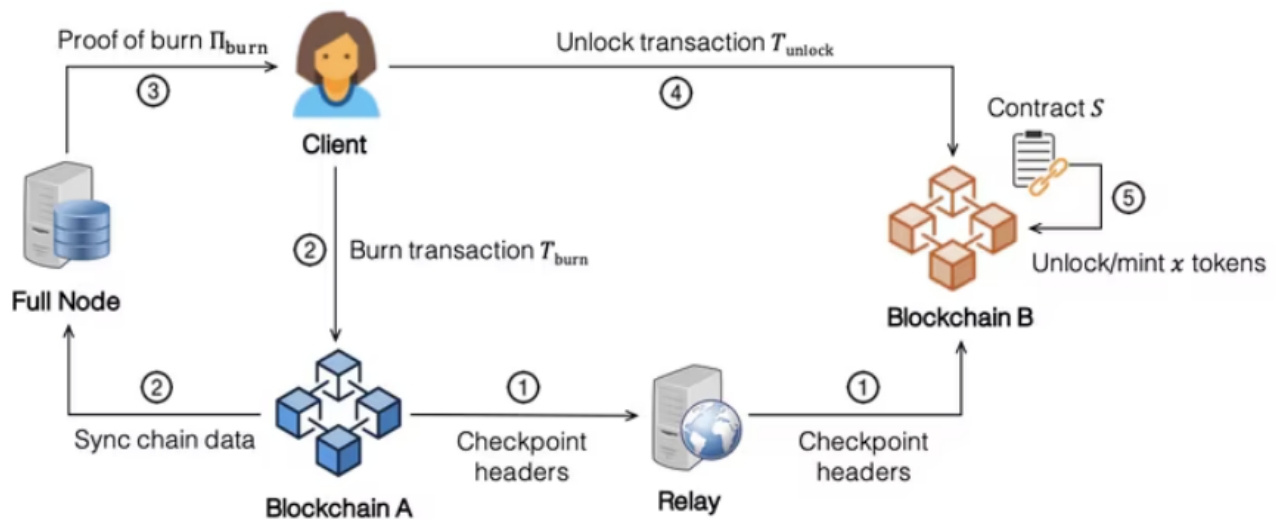
Performance degrades after about 200 validators

Polkadot - 1.5K tps, dependent on the number of parathread slots available. Polkadot aims for about 1000 validators in the relay chain.

Other Solutions

Harmony

Harmony's bridges can connect any Proof-of-Work and Proof-of-Stake chains. Our FlyClient architecture is fully trustless and highly gas-efficient. Currently, there are bridges for Ethereum and Binance Smart Chain.

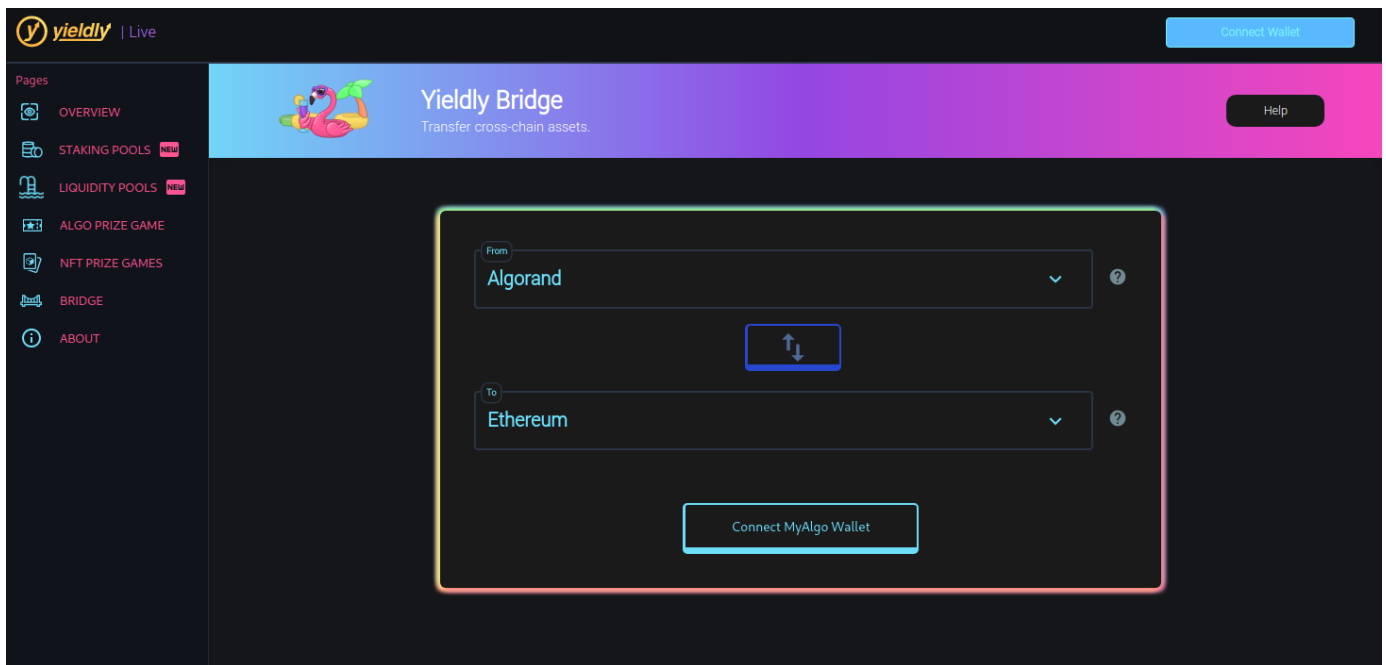


	Harmony	Ethereum	Ethereum 2	Cosmos	Polkadot
Tx Finality	2 seconds (1 block)	6 mins (25 blocks)	12.8 minutes (64 blocks)	7 seconds (1 block)	12 seconds (1 block)
Validators	1,000	>7,105	8,192	120	200
Tx Fees	\$0.000-001	\$0.304	\$0.000-002	\$0.000-1	\$0.000-001
Mainnet Launch	June 2019	July 2015	Dec 2020	March 2019	June 2020
Shard Size	250 nodes	N/A	128 nodes	125 nodes	100 nodes
Annual Issuance	3%	1%	2%	7%	2.5%
Shards	4 shards	1 shard	64 shards	15 chains	100 shards

Yieldly (Algorand)

Yieldly Finance (<https://yieldly.finance/>)

"Yieldly (<https://www.algorand.com/ecosystem/use-cases/yieldly>) has built the first set of DeFi smart contracts native to Algorand. By bringing the power of DeFi to Algorand, Yieldly lets users stake, pool, and swap ASA assets. "



Article from Vitalik about the danger of bridges

I don't expect these problems to show up immediately. 51% attacking even one chain is difficult and expensive. However, the more usage of cross-chain bridges and apps there is, the worse the problem becomes. No one will 51% attack Ethereum just to steal 100 Solana-WETH (or, for that matter, 51% attack Solana just to steal 100 Ethereum-WSOL). But if there's 10 million ETH or SOL in the bridge, then the motivation to make an attack becomes much higher, and large pools may well coordinate to make the attack happen. So cross-chain activity has an anti-network-effect: while there's not much of it going on, it's pretty safe, but the more of it is happening, the more the risks go up.

https://old.reddit.com/r/ethereum/comments/rwojtk/ama_we_are_the_efs_research_team_pt_7_07_january/hrngyk8/

(https://old.reddit.com/r/ethereum/comments/rwojtk/ama_we_are_the_efs_research_team_pt_7_07_january/hrngyk8/)