Lowdown on Appchain Networks

Simon Brown

Follow

--

1

Listen

Share

This is high level overview and comparison of prominent multi-chain networks, including Cosmos and Polkadot, as well as newer networks such as Polygon Edge, Avalanche and Celestia.

I wrote this material in August based on research I was doing at the time into application specific chains aka “appchains”. I had been reading a lot of material around modular architecture and appchains, and I wanted to take a deep dive into that area.

In doing so, I became increasingly interested the Cosmos ecosystem and the technology behind it. Recently I read the Cosmos Hub whitepaper and it has increased my interest, as it addresses many of the issues of the current iteration of Cosmos, and proposes improvements that future proof the entire ecosystem.

The following material covers Polkadot, Cosmos, Avalanche Subnets, Polygon Edge and Celestia, but with particular attention paid to Cosmos, as I personally found it particularly interesting.

Polkadot

Polkadot ostensibly provides the best of both worlds (in terms appchains vs. rollups), because it provides security for its parachains via a highly secure “Relay Chain”, so that the parachains don’t have to rely entirely on their own security. Parachains use custom VMs, built in any language, optimized to very specific use cases, but can also leverage the security of the Relay Chain. The Relay Chain in Polkadot assigns a subset of validators to each Parachainfor each epoch, and this subset of validators validates the block for a given slot for the parachain to which they are assigned. The parachain block is validated against a consensus / fork-choice rule that is specified when the parachain is first registered with the system.

Currently the Relay Chain has 297 validators, with plans to extend this to 1,000over time. The set of 297 validators can theoretically change on a daily basis as validators are elected from the waiting pool every day. This is in stark contrast to Ethereum which has 415,409 validators at the time of writing.

The Relay Chain measures ~ 1,000 TPS, with no theoretical upper bound on the throughput of parachains (given that they can specify their own fork-choice rule). That being said, one of Polkadots stated research goals is to arrive at an average standard of 1,000 TPS for parachains.

An important point to be aware of is that the number of validators on the network quickly reaches the point of diminishing returns, whereby having 1,000 independent and geographically dispersed validators is every bit as secure as having 1,000,000 validators. The cost of compromising hundreds of independent validators through coercion or cyber attacks is infeasible, and the cost of economic attack does not depend on the number of validators, but rather the market capitalization and even distribution of the native asset among holders and validators.

However, in terms of scalability, when Ethereum implements full data-sharding via enshrined PBS and danksharding with data-availability sampling, this logic inverts. With data-sampling, the more nodes you have on the network, the more powerful and secure the data-sampling becomes, allowing the network to handle far bigger blocks (danksharding aims for 32MB blocks), which will allow a far greater number of rollups, and allow the rollups to process far more transactions. At this point, I see Ethereum as a having a technical advantage over heterogeneous multi-chain networks such as Polkadot.

Decentralization and Democratization

According to the documentation: “The minimum stake that is necessary to be elected as an active validator is dynamic and can change over time. It depends not only on how much stake is being put behind each validator, but also the size of the active set and how many validators are waiting in the pool.

”

As of the time of writing, theminimum amount of DOT required to stakein order to become a validator is 1.8573M DOT, which equates to approximately $15,863,383 USD. Due to the Polkadot nominated proof-of-stake system (nPoS), this largely comes from DOT holders that delegate their DOT to validators for a pro-rata share of block rewards and transaction fees. As of the time of writing, the total number of validators on the network (both elected validators and those in the waiting pool) is 994.

In terms of nominators, only the top 256 (at the time of writing) actually receive any payouts from validator rewards. That means that a nominator has to delegate a minimum of ~ $62,000 USD in order for it to be economically viable. This figure is derived from the value of the minimum threshold of DOT required for staking divided by the maximum number of nominators that can delegate (i.e. 15,863,383 / 256).

This represents a higher barrier of entry to staking and validating than exists on Ethereum. Staking on Ethereum requires 32 ETH (~ $52,000 USD at the time of writing), which is less than is required for a single nominator on Polkadot.

It is worth noting that it is stated that the Relay Chain can support amaximum of approximately 100 parachains. These parachains must bid for tenancy on the relay chain, and can bid up to 2 years tenancy, after which they must bid again in an open auction. There are some “slots'' on the Relay Chain that allow smaller chains to bid in an open auction on a pay-as-you-go basis. These smaller chains are referred to as “parathreads”. It’s not clear how many parathreads will be supported, what the fees will be, or indeed how much of a bottleneck the relay chain will be on throughput (or at least I couldn’t find this information anywhere).

Cosmos

Cosmos does not have shared security, though this is on their roadmap, referred to as Interchain Security. For the time being it means that each zone is entirely responsible for their own security.

As the Cosmos SDK allows for easy plug and play of various core modules, most zones in Cosmos adopt a proof-of-stake sybil-resistance mechanism. As consensus is based on Tendermint, this means that security is predicated upon an honest-majority assumption, whereby ⅔ of the validators must be honest in order to maintain liveness and safety.

According to the documentation on Interchain Security:

“The security of a network is often described as a function of the cost for attacking that network. In Tendermint consensus we target ⅓ and ⅔ of locked stake for various guarantees about liveness and correctness. This means that in order to do any of a variety of attacks against the network, you would need to acquire ⅓+ or ⅔+ of all stake. The crude way to calculate the cost of an attack is to take the quantity of tokens needed to achieve these proportions and multiply it by the current market price for that token. We’ll call this the Cost of Corruption.”

To better understand what this means in a real-world setting, I wrote a quick script to gather and analyze data on the validator sets of various zones. The objective was to understand how many validators in each zone would have to be compromised in order to affect the security of the entire zone. A sample of the results are displayed in the chart below:

As you can see, based on the percentage of staked native asset for each validator on the zone, the number of validators required to compromise the zone is alarmingly low in most cases. In this case, I’m considering the zone to be compromised if > ⅓ of the validators can collude to create a liveness fault on the network.

For certain zones, it requires only the top 2 to 3 validator nodes (by amount staked) to compromise the network. Taking a subset of the above data and adding in the market cap., this becomes even more alarming.

Obviously there is some security in the fact that these are sovereign chains, therefore disincentivizing any take-over, as the chains can simply be forked to reclaim any stolen assets.

This should not be regarded as a robust solution though in my opinion, for a number of reasons. For one, Cosmos’s interoperability means that these assets can (and likely will) be transferred to other zones such as DEXs (e.g. Osmosis for example).

If the chain that originates these assets forks or undertakes a deep re-org or re-genesis, it’s unclear what downstream effects it could have on assets that have previously been transferred to other chains, or what effect it can have on the light clients of other chains. Therefore, “social slashing”, or forking the chain to recover assets, is not a reliable or robust security mechanism in the long term.

The problem is that the challenge of incentivizing validators to provide security to a chain can lead to a low security budget for many chains, even for those whose native asset enjoys a significant market capitalization.

Below is a chart that is derived from taking a sample of zones within the Cosmos ecosystem. The sample size is 15 and represents about a third of all the zones currently active. While there are a number of zones with a much higher security budget, this sample demonstrates that a large number of zones within the Cosmos ecosystem have relatively low security compared to larger L1 networks.

This can have serious consequences and real-world implications. An example of this Gaming blockchain Axie-Infinity lost $540M USD in March of 2022 due to a compromise of their network. While their chain was not a Cosmos zone, it is comparable in that it is a sovereign appchain.

An article that summarizes the post-mortem states that:

“after successfully infiltrating Ronin’s systems through the fake job ad, the hackers had control of just four out of the nine validators

— meaning they needed another in order to take control.”

This presents a challenge to new networks to bootstrap security, initially moving from a PoA network to a progressively more decentralized PoS network, but the data clearly indicates that this has been a challenge for smaller networks.

In trying to understand the challenges to growing a validator set enough to maintain a robust security budget for the network, it is important to examine the incentives for validators to join the network.

In order to attract validators to stake and validate, the rewards for doing so must be substantial, especially at the beginning. This requires a high level of issuance / inflation to act as an incentive for validators to join the network. This means that the native asset holders that don’t stake, risk the asset becoming diluted and possibly losing value over time.

There is an argument that the growth in utility value over time will offset the effects of inflation and the dilution of unstaked assets. That being said, a high inflation rate strongly incentivizes people to stake on the network to counteract dilution. This in turn reduces the circulating supply, which theoretically pushes up the price of the native asset but also in theory creates a zero-sum game, whereby more assets will become staked and locked, increasing the dilutionary effect on the tokens in circulating supply.

At a certain point, once the majority of assets on the network are staked, the dilutionary effect on the unstaked assets will outweigh the growth in utility value which positively impacts the price. This reduces the value of the native asset, which in turn undermines the security budget for the network. In worst cases, the negative effect of this sort of inflation can reach an inflection point which can trigger sudden and significant sell-offs. There have been precedents for this effect to cause networks to fail, and some of these examples have been explored in detail by Polynya.

Interchain Security

While the economic challenges of bootstrapping a validator set may not be an issue for private / consortium chains, it is certainly an issue for public chains, and this is the main impetus for the Interchain Foundation to move to develop interchain security. The specification describes interchain security as:

“Interchain Security is a new shared security primitive that has implications for the security and scalability of single blockchains like the Cosmos Hub as well as the potential to dramatically lower the barrier to running secure public blockchains for new applications. It could be thought of as a competitive configuration to sharding and put the Cosmos Hub on par with Eth 2.0 or Polkadot in terms of their security offerings to applications included in their environment.”

Interchain Security allows for a provider chain (like the Cosmos Hub), to create blocks for a consumer chain. The provider chain facilitates a subset of its validators to validate blocks on both the Cosmos Hub and some zone (i.e. The consumer chain). These subset of validators run two nodes, one for the Cosmos Hub and one for the other zone they are validating. They would then receive fees and block rewards on both the Cosmos Hub and the consumer chain zone.

Interchain Security greatly improves the ability to co-ordinate and onboard validators. Validators will not need to acquire and stake the native asset of a chain in order to participate as a validator. Instead they can stake ATOM on the Cosmos Hub (or any hub that provides interchain security) and therefore can have ATOM delegated to them from ATOM holders.

Furthermore, Interchain Security will allow many more validators to join the Cosmos Hub. Currently there is a maximum of 150 validators on the Cosmos Hub due to the limitations of the Tendermint consensus protocol. While this limit remains for validating the Cosmos Hub, many more validators can join the pool with a view to explicitly providing security for other chains. This will be an opt-in basis, and as such, it will still be up to the individual chains to provide incentives that maintain a healthy security budget for that particular chain.

There are other open questions that remain to be answered, and may only be answered as Interchain Security is rolled out and adopted by the Cosmos ecosystem. Questions arise over the governance of individual chains, and what implications that has for validators. Also, there may be considerations with regards to how many child chains it is feasible and safe for a validator to provide validation services to.

Interoperability as a weakness of Ethereum

One of the key weaknesses of Ethereum compared to networks with enshrined interoperability such as Cosmos or Polkadot, is the lack of a single, secure interoperability protocol.

There are a wide variety of different solutions that dapp developers and users can choose from in order to facilitate cross chain communication and asset transfer, but the space is fragmented between these various solutions, and it is left to the developer and the end-user to measure the risk involved in using one bridging solution over another bridging solution.

There has been approximately 2 billion USD stolen from compromised bridges in the past twelve months alone. Below are some of the high profile security incidents:

Note that these breaches apply to bridges that bridge Layer 1s, as opposed to bridges that are employed by Layer 2 rollups, which rely on validity proofs or fraud proofs, a distinction that is explained in detail by Schmid et al. Schmid also underlines the caveat that bridges are only as secure as the chains they bridge, which applies to all protocols regardless of the interoperability protocol employed.

Multi-chain networks such as Cosmos and Polkadot have interoperability enshrined at the protocol level, and to date, have not suffered any breach of the protocol that routes transactions or messages between chains. Due to the enshrined interoperability, there are a large number of connections between different chains within these ecosystems. Take for example the chains on Cosmos:

As you can see from the chart below, nearly every sovereign chain within the Cosmos ecosystem has a number of connections to several other chains. Some of these connections represent connections to DeFi zones, such as Osmosis, and other connections are the zones that address specific concerns, such as Starname, which is used for maintaining human readable names that resolve to Cosmos assets, or Cheqd, which provides support for Verifiable Credentials.

Unlike the multitude of interoperability protocols that serve as bridges between Ethereum and other protocols, Cosmos IBC allows for more than just token transfers, but allows zones to fully leverage applications and smart contracts on other networks as well as just transferring tokens between them.

According to the documentation:

“Chains having enabled ICS-27 can programmatically create accounts on other ICS-27-enabled chains and control these accounts via IBC transactions, instead of having to sign with a private key. Interchain accounts contain all of the capabilities of a normal account (i.e. stake, send, vote) but instead are managed by a separate chain via IBC”.

Comparison to Newer Networks and Alternatives

Avalanche Subnets

Avalanche allows for creating sovereign blockchains called subnets. A subnet requires at least five validators. Validators on a subnet will need to also perform validation duties on the main P-Chain as well (that is, they will need to be validators on both the P-Chain and and the subnet). Validators can be created for the chain specifically, or they can be incentivized to become validators from the existing validator network.

Security

It is important to note that to become a validator on Avalanche, 2000 AVAX needs to be staked. At the time of writing, 2000 AVAX = $44,512 USD. This means that at least $222,563 USD is required in order to launch a subnet with one’s own validators. The alternative is to try to incentivize validators from the existing validator pool.

Validators earn transaction fees from the subnet they are validating on. There is no staking on subnets at the moment. This makes subnets essentially PoA systems, in which validators that stake and validate on the P-Chain, validate blocks on subnets and collect transaction fees in return.

Sovereignty

Avalanche subnets can be self-sovereign chains, according to theirFAQ:

“No. Subnets have their own state and execution thread. So it does not share the processing, TPS, or networking with the Primary Network. Thus enabling lower latency, higher transactions per second (TPS), and lower transaction costs.”

It is possible to deploy a custom VM, or a ready-made VM that can form the basis for a variety of use-cases, including EVM, AvalancheVM, SpacesVm (key/value storage), BlobVM (binary storage), TimestampVM (a minimum viable VM). There are also others in development.

Interoperability

Interoperability is something that Avalanche falls behind in. Again, from the FAQ:

“There is currently no built-in support for intra-Subnet cross-chain transactions. Support for cross-Subnet transactions is on the roadmap for later in 2022.”

There is no bridge from a subnet to the Avalanche network, though this is currently under development. In the meantime, subnets can build their own bridge or use a 3rd party solution to communicate with C-chain and other Subnets.

Polygon Edge and Polygon Supernets

Polygon Edge is described as “a modular and extensible framework for building Ethereum-compatible blockchain networks, sidechains, and general scaling solutions.”

Polygon Edge uses IBFT (Istanbul Byzantine Fault Tolerant) consensus mechanism, either as a PoA or PoS network.

Interoperability

Polygon Edge uses a bridging solution called “ChainBridge” for cross chain token transfers. ChainBridge is built by ChainSafe and is described as “a modular multi-directional blockchain bridge supporting EVM and Substrate compatible chains”

.

Sovereignty

Polygon Edge is EVM compatible, no other runtime is supported. This means that no custom VM can be used, and functionality must be expressed through smart contracts. Polygon claims that the VM can be extended / adapted through the use of “runtime plugins” but no documentation on this could be found. Polygon Edge supports PoS and is fully parameterizable.

Supernets

Supernets leverage Polygon Edge but offer the ability to quickly deploy a Polygon Edge blockchain without having to supply or source validators or to maintain infrastructure such as node providers, block explorers, RPC providers etc.

With Polygon Supernets, the validator set is sourced from professional validators who must stake a minimum of 20,000 MATIC on Ethereum mainnet in order to be validating the network (approximately $16,000 USD at the time of writing).

At the time of writing, there are more than 35 networks having been built using Polygon Edge and more than 110 projects looking to migrate to or build on Polygon Supernets.

Supernets are not designed to allow end-users to deploy their own arbitrary smart contracts as they would on the mainnet, the only smart contracts are your own.

Celestia

Celestia is data availability that allows other chains and rollups to anchor into.

Celestia is different from other Layer 1 blockchains in as far as it doesn’t contain any execution layer. The base layer simply accepts data blobs, orders them in the sequence they arrive in, and facilitates data availability sampling to guarantee that the data is available to all who need it. This allows chains to leverage Celestia as a DA layer, and just focus on execution.

Celestia is built using the Cosmos SDK, and uses the Tendermint consensus algorithm. There is some state and execution on the chain, but only the minimum required to maintain PoS. This is somewhat similar to the notion of “hub minimalism” in Cosmos, with one key difference, Celestia doesn’t interpret any of the data it receives in transactions, it simply records it.

By acting solely as a specialized data availability layer, Celestia can be much cheaper than Ethereum in it’s current phase, where data is posted as calldata. Rollups on Celestia can continue to use Ethereum as a settlement layer if they want to, posting validity proofs and fraud proofs, while using Celestia for data availability.

The reason Celestia can offer far cheaper data availability is that it has engineered a sophisticated light client data sampling, whereby each node on the network only samples a small portion of the data. If data is missing or corrupt, they can provide data availability fraud proofs. This is very similar to the design of full danksharding with data availability sampling.

This approach scales with the number of nodes added to the network, and thus the more the network grows, the more data it can handle and the cheaper the fees become. Furthermore, as the network grows to be able to handle more data, the greater the block size of the chains that are using it can become, which of course has effects on the scalability of those chains (more TPS, lower node resource requirements, faster finality).

Celestia claims that it can handle any number of rollups or blockchains. Each chain / rollup has its own “namespace” inside Celestia’s state tree. This is achieved by using a Namespaced Merkle Tree, which basically dedicates top level sub-trees within the state tree to specific chains.

Rollups that are built on top of Celestia can be either Ethereum based rollups or Celestia based rollups (sovereign rollups).

Ethereum rollups can use Celestia as a DA layer, while using Ethereum as a settlement layer by posting validity proofs / fraud proofs to Ethereum and posting data blobs to Celestia. Celestia subsequently posts attestations to the data to Ethereum, which contains signatures and proofs that attest to the data on Celestia.

This type of rollup is what Celestia refers to as “Celestiums”, and the posting of data attestations to Ethereum is handled by it’s Quantum Gravity Bridge.

The other type of rollup that can be deployed on Celestia is aSovereign Rollup, and works slightly differently. These types of rollups have a single sequencer or operator, like Etheruem rollups, but also have other nodes on the network as well. The nodes on the rollup network can be either full nodes or light nodes.

Rollup full nodes are nodes which download the data of blocks posted to Celestia by the operator. They subsequently verify all the transactions in the block, and update their local state accordingly. If a full node detects any invalid transaction, it rejects the block, and optionally creates a fraud proof in the case of optimistic rollups.

Light nodes don't download all the data, but can query full nodes for individual transactions, account balances etc. They can also verify transactions by verifying the associated merkle proofs and verifying the validity proof in the case of zk-proofs.

This approach is different from Ethereum rollups, whereby the validity proofs and fraud proofs are verified by on-chain smart contracts. Celestia native rollups rely on an honest minority of full nodes to verify the data and to take over as rollup operator if need be. From the Celestia blog:

“Fraud and validity proofs also work similarly to how they would work in a layer 1 blockchain. Fraud proofs are gossiped to clients directly via the peer-to-peer network, and validity proofs are simply included with the block header.”

To make it easier for developers to develop sovereign rollups, Celestia has releasedOptimint, which is a sovereign rollup based on the Cosmos SDK, which aims to make it very easy for developers to create sovereign rollups on top of Celestia.

Going a step further in thinking about a sovereign rollups on Celestia, it is possible to create a sovereign rollup whose only function is to verify the validity of fraud proofs of other rollups. This concept is known as a settlement rollup

. To use this settlement rollup, other rollups would still use Celestia as a DA layer, but would post validity proofs and fraud proofs to the settlement rollup. This concept is discussed in more detail on the Celestia forums, and is also is architecture of the proposed Cevmos chain.

Cevmos is an acronym for Celestia — EVMos — CosmOS. Cevmos acts as a settlement layer for Celestia rollups, by using Optimint, which is a drop-in replacement for Tendermint, and Evmos, which is a Cosmos SDK chain with an in-built EVM.