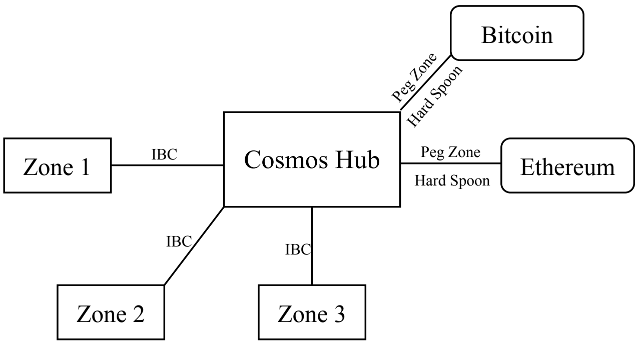
Cosmos Network Economic Design Analysis

Cosmos Network is regarded as Blockchain 3.0 ecosystem with technical innovations of solving problems faced by other blockchains. The vision of Cosmos Network is to create an Internet of Blockchains, a network of blockchains able to communicate with each other in a decentralized way.

In this article, we would like to analyze the economic design of Cosmos Network, firstly understand its structure, then assess its performance from an economic perspective, finally evaluate its pros and cons and offer some takeaways for the blockchain start up CertiK.

Part I: Cosmos Network Economic Design Overview

To my understanding, the whole economic design of Cosmos Network can be demonstrated as below.



Open Source Platforms:	Tendermint
	Cosmos SDK
Protocols:	IBC
	Peg Zone
	Hard Spoon
Tokens:	Atoms
	Photons
	Whitelisting Tokens
Major Participants:	Validators
	Delegators

Further explanations of the above concepts are as follows.

- Tendermint

Tendermint is a public platform which provides web-server, database and supporting libraries for blockchain applications. It consists of two chief technical components: a blockchain consensus engine called Tendermint Core and a generic application interface called Application Blockchain Interface (ABCI).

- Cosmos SDK

Cosmos SDK is a generalized framework that simplifies the process of building secure blockchain applications on top of Tendermint as well as expedites the process for developers to create their own applications on their own blockchains.

- Inter-Blockchain Communication & Peg Zone & Hard Spoon

Inter-Blockchain Communication (IBC) is a protocol to connect heterogeneous blockchains to transfer values or data to each other within Cosmos Network.

Unfortunately, neither Bitcoin nor Ethereum have finality guarantees whereas IBC only works in the situation in which both the starting and ending chains have finality settlement.

Peg Zone and Hard Spoon are the solutions to this problem. They are protocols which bridge zones within Cosmos to external chains such as Bitcoin or Ethereum.

The difference between Hard Spoon and Peg Zone is that a Hard Spoon occurs when a new minted cryptocurrency launches on a different new chain with the replicated account balances. It ends up with two cryptocurrencies that run parallel on different blockchains, where each has its own value, can be used for staking and is also tradeable. Hence, Peg Zone deals with a sidechain while Hard Spoon is for a new blockchain.

- Cosmos Hub & Zones

The Cosmos Hub is the first blockchain of the Cosmos Network with the goal of providing connectivity, consensus, security and preventing double spending.

Zones are regular heterogenous blockchains using IBC to communicate one another via Cosmos Hub.

- Atoms & Photons & Whitelisting Tokens

Atoms are the native staking token of the Cosmos Hub. Atoms are license for the holder to vote, pay fees, validate, or delegate to other validators. Atoms are designed to secure the network with an annual inflation between 7% and 20% depending on the percentage of the atom supply that is staked.

A secondary token Photon is planned to be introduced with the intent to pay fees and block rewards. Photons are highly liquid and have an inflation rate of asymptotically zero.

There are plans to whitelist other cryptocurrencies (e.g. bitcoin or ether) for paying transaction fees, once those tokens become available on the Cosmos Hub.

- Validators & Delegators

Validators verify transaction within a blockchain to secure the network. They commit new blocks, vote on blocks of transactions, get rewarded proportional to their stake if the majority of the network agrees , risk losing stake if they try to cheat, e.g. by voting on two different blocks of transactions at the same time. The Cosmos Hub will have 100 validators, overtime it may increase to 300 according to its predefined schedule.

Delegators deposit tokens in smart contracts specifying the validators whose influences in the network they want to increase. Delegators act as safeguards of validators. If validators misbehave, their delegators will move their atoms away, thereby reducing their stake.

Note: *We will elaborate the concepts of Cosmos Hub, Zones, Atoms, Photons, Validators, Delegators in the next two parts from an economic perspective. Because this is an article with focus on economics, for more general information of each concept, please see the links in reference part.*

Part II: Cosmos Network Economic Design Analysis

1. Game Theory Analysis of Tendermint

A rational individual always chooses the optimal risk-adjusted option by taking into account decisions of others. However, this may sometimes lead to an unfavorable result.

The prisoner’s dilemma is an example, where two rational and independent players must choose between cooperation and conflict to arrive at what is perceived as the best outcome. In this scenario, two prisoners, let’s say Alice and Bob, are being interrogated separately. If both confess, each is sentenced to eight years in prison; if both deny their involvement, each is sentenced to one year. If just one confesses, he/she is released but the other is sentenced to ten years.

		Bob	
		Deny	Confess
Alice	Deny	-1, -1	-10, 0
	Confess	0, -10	**-8, -8**

Payoffs to: (Alice, Bob)

The conclusion is that Alice and Bob will be sentenced to eight years. The most favorable strategy for both is to deny so that they two only are sentenced to one year. However, neither is aware of the other’s strategy and without certainty or trust that one will deny, both will likely to confess and, as a result, receive eight years.

So, in a decentralized network with more uncertainty, how to avoid the similar unfavorable result from the perspective of game theory?

One of the reasons why Bitcoin has succeeded is that its network design complies with game theory. The economic logic is to create a balanced rule of risk and reward which participants can behave honestly to choose the optimal solution aligned with self-interest, while at the same time still maintain the consensus of a system.

Under the Bitcoin Proof of Work (PoW) algorithm, the rewards will be given to the miner who firstly solves the puzzle and adds the block to the longest blockchain, which avoids the double spending issue. Also, the maximal penalty for incorrect behavior which can potentially far outweigh mining rewards defined for correct behavior. Nevertheless, there are many problems of PoW such as hardware cost and huge electricity consumption. Proof of Stake (PoS) addresses the problems that PoW faces by attributing mining power to the proportion of tokens held by a miner, which transits the block validation function from miners to validators.

Tendermint is a consensus based on Proof of Stake (PoS) with a few its own features.

- Byzantine Fault Tolerance. Tendermint tolerates only up to 1/3 or machines failing arbitrarily including explicitly malicious behaviors.
- Consistency-Prioritizing. The design behind Tendermint prioritizes safety and consistency over liveness and flexibility.
- Instant Finality. There is no need to allow for block $n + i$ where $i \geq 1$ to commit, when block n itself hasn’t yet committed. This allows for faster provable transaction commits for SDK and faster inter blockchain communication.
- High Performance. Tendermint has a block time on the order of 1 second and handles up to thousands of transactions per second.
- Language Diversity. Tendermint supports state machines written in any programming languages.

Additionally, here we would like to explain Byzantine Fault Tolerance (BFT) in case you are not familiar with this concept. BFT is a system to resist the failure derived from the Byzantine Generals' Problem, which is a dilemma of how a group of Byzantine generals agree on their next move via communication.

The dilemma assumes that each general has its own army and that each group is situated in different locations. Three requirements must be met for their next move. First, each general has to decide either attack or retreat; Second, the decision cannot be changed once made; Third, all generals have to agree on the same decision and execute it in a synchronized manner.

The aforementioned communication problems are related to the fact that one general is only able to communicate with another through messages forwarded by a courier. Therefore, there is a potential problem that messages can be delayed, maliciously destroyed or lost. In addition, even messages are successfully and correctly delivered, one or more general may choose to act oppositely to confuse other generals, leading to a failure.

If we apply the dilemma to the context of blockchains, each general represents a network node, and the nodes are supposed to reach consensus. The majority of participants within a decentralized network have to agree and execute the same action to avoid the failure. BFT is such a system able to continue operating even if some nodes fail or act maliciously.

2. Utility Analysis of Cosmos Tokens

Cosmos tokens can be considered as a commodity, which have two identified types of value: use value and exchange value, according to Marxian economic terminology. Use value is "want satisfying power" which is based on the utility of a commodity; Exchange value is "the amount of goods and services in the market in exchange for a particular thing" which can be indicated by the price of the commodity. We can define the economic security of blockchain network as the amount of money needed to be spent in order to attack the system, which is more related to the exchange value.

There is a dilemma to keep balance of the network security and token liquidity by using the single-token model. On the one hand, a large amount of the token should be staked to guarantee the security of the network. On the other hand, an amount of the token should be used for transaction fees, which will increase the liquidity but weaken the security of the system as it makes easier for attackers to obtain enough tokens required to attack the network. In a word, a single token with both use value and exchange value for staking and exchanging purposes cannot perfectly coexisted in this scenario.

Instead, Cosmos uses the multi-token model, in which Atom is used primarily for staking while Photon is used to pay fees or used as a currency. Also, there are plans to whitelist other cryptocurrencies (e.g. bitcoin or ether) for paying transaction fees, once those tokens become available on the Cosmos Hub.

3. Incentive Analysis of Atom Holders

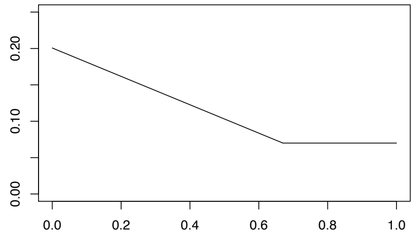
We want to explore how economic specifications incentivize a network of atom holders, i.e. validators and delegators. First, we will introduce the atom inflation method. Next, we will make incentive analysis of being a delegator and validator respectively.

3.1 Atom Inflation Method

Cosmos uses inflation to incentivize the staking of atoms. New atoms are created per block and distributed to holders participating in the consensus process. The number of new atoms created per block depends on the percentage of the atom supply that is staked in the network. The target rate of atoms to secure the network is at least 2/3 of the total atom supply. If fewer atoms are staked, supply via block rewards increases up to a ceiling of 20% annualized inflation of the total supply. If more atoms are staked, supply decreases down to a floor of 7% annualized inflation.

Let's use *i* as annual inflation rate, *s* as the percentage of atoms staked. The relationship between *i* and *s* is shown below, both in formula and graph.

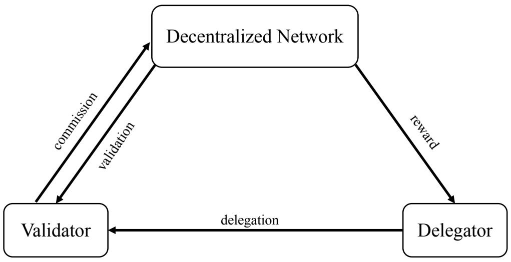
$$i = 0.07 \text{ when } s > 0.67$$
$$i = 0.07 + 0.13 * 1.5 * (0.67 - s) \text{ when } s \leq 0.67$$



Overall, from the above graph, we can see that more atoms staked lead to lower inflation rate, which means that the value of atoms will decrease if fewer atoms are staked. This atom inflation method provides an incentive for atom holders to put more atoms at stake to maintain the value of atoms as well as the security of the network.

3.2 Validator and Delegator Incentive Analysis

The simplified overview of the role of validators and delegators is pictured below.



A rational investor chooses between delegator and validator with the higher expected return. We build a qualitative incentive model with four parts like below and will explain major components of each part.

$$\textit{Expected Return} = \textit{Rewards - Costs - Risks}$$

As for a validator,

Rewards
A Validator can set a commission rate for block rewards, provisions and fees they gain before the distribution of the rest portion will go to the delegator.

- Staking Rewards. Rewards from staking vary based on the amount of atoms staked, the supply of staked atom, block time interval, fee revenues, validator uptime, re-staking behavior, atom token price, etc.

- Block Provisions. Validators receive additional atoms from continuous inflation. The inflation rate depends on the total amount of atoms staked.
- Transaction Fees. Transaction fees are split among validators and delegators based on their stake.

Costs

- Infrastructure Cost. A secure system is required to guarantee a continuous operation.
- Operation Cost. Building and maintaining a well-performing network requires technical expertise, time and management skills.
- Opportunity Cost. To protect against a validator attacking the network and then immediately withdrawing the stake, there is a 21-day un-bonding period. When locked, participants lose the opportunity to invest in other assets.
- Delegator Cost. To attract more delegators to pick themselves as validators, validators may invest on areas such as marketing, customer support, business development, legal, etc.
- Network Tax. Network tax which goes into a reserve pool is used to maintain the security of network.

Risks

- Liquidity Risk. As this is prevalent in most PoS algorithm, there is often a lockup period associated with staking to prevent attacks. Without the lockup period, a malicious party could attack the network and withdraw their stake immediately leaving no chance for the protocol to punish the offense.
- Slashing Risk. It is the risk of losing deposited tokens due to not following the network protocol.

As for a delegator,

Rewards

- Staking Rewards. A validator earns the commission. The rest goes to the delegator.
- Block Provisions. A validator earns the commission. The rest goes to the delegator.
- Transaction Fees. A validator earns the commission. The rest goes to the delegator.

Costs

- Re-stake Cost. If delegators choose to re-stake rewards to let them compound, they have to manually withdraw and delegate rewards again because there is no option of an automatic way for now. The cost fees of re-stake rely on network condition, i.e. fee level, effective inflation rate and delegated amount.
- Opportunity Cost. The same as a validator.
- Network Tax. The same as a validator.

Risks

- Liquidity Risk. The same as a validator.
- Slashing Risk. The same as a validator.

Other Factors both for a Validator and a Delegator

There are other not purely financial motives for choosing to between a validator and a delegator. These include improving decentralization of the network, supporting particular governance parties, regulatory implications, user experience, benefits of staking with a validator on multiple networks, comparison between token borrowing rates and staking return rates, considerations of validator set size or minimum staking balance, other value-added services that a third-party delegation service may provide.

In summary, a table of incentives of validators and delegators is shown below.

	Validators	Delegators
Rewards	Commission from Staking Rewards Commission from Block Provisions Commission from Transaction Fees…	Staking Rewards Block Provisions Transaction Fees…
Costs	Infrastructure Cost Operation Cost Opportunity Cost Delegator Cost Network Tax…	Re-stake Cost Opportunity Cost Network Tax…
Risks	Liquidity Risk Slashing Risk…	Liquidity Risk Slashing Risk…
Other Factors	Improving decentralization of the network, Supporting particular governance parties, Regulatory implications, User experience, Benefits of staking with a validator on multiple networks, Comparison between token borrowing rates and staking return rates, Considerations of validator set size or minimum staking balance, Other value-added services that a third-party delegation service may provide…	

4. Economic Principle behind Network Security

Blockchain network security is significantly crucial. Validators in Cosmos need a network-connected servicer to constantly produce and sign new blocks. So, if attackers can gain control over the infrastructure and setups, they can attack the network.

Apart from using a multi-token model and atom inflation method to address this issue, a few points are elaborated here.

The positive correlation between token price and infrastructure investment is a behind economic principle of maintaining network security. Specifically speaking, rising price of a token drives higher revenue, resulting in more money being spent on network infrastructure. Higher amount of money invested in the infrastructure will increase the security of the network as it becomes more expensive and harder to attack it.

One thing should be mentioned that, a portion of transaction fees goes into a reserve pool as network tax, planned to be used to increase the security and value of Cosmos Network.

Nonetheless, this doesn’t mean that no attack can be executed. Higher price of a token means more value is secured by the network, which also indicates that the profitability of a successful attack increases though the cost correspondingly increases. Therefore, it is important for validators to build a secure infrastructure. This includes using HSMs (Hardware Security Modules), having physical security in data centers, having a resilient sentry node setup, securely generating keys, getting security audits done, etc.

Part III: Cosmos Network Pros & Cons Analysis, and Takeaways for CertiK

1. Multi-Token Model

Pros

Multi-token model solves the dilemma of keeping balance of the network security and token liquidity as discussed before.

Cons

How to determine the exchange rate of one token over another may be an issue. Specifically, Cosmos is supposed to decide how much photons is equal to one atom. Also, multi-token model may be less convenient than single-token model in practice.

Takeaways

As far as I am concerned, the pros of multi-token model outweigh the cons. Currently, CertiK uses CertiK token as its single token. If it is possible, I would personally suggest to use multi-token model based on previous analysis.

2. Governance

Pros

As stated in Cosmos Network Whitepaper, validators and delegators on the Cosmos Hub can coordinate upgrades and vote on proposals, amendments as well as policies. Each zone can have its own constitution and governance mechanism. From my point of view, I am positive about the overall design of the governance system because it achieves democracy in the Cosmos Hub and gives flexibility to zones.

Though the specific plan of the governance system hasn't been published, there are some ideas that may inspire governance proposals. For example, reduce downtime from 18 hours to 12 hours, increase the severity of the slashing, increase double sign slashing from 5% to 20%, speed the inflation to 4x faster, etc.

Cons

Regarding the governance of major participants of Cosmos network, I personally want to raise a concern concerning the incentive model of validators and delegators. In my opinion, as you can see from the table summarized in part II, the incentive to be a delegator on average is more than that to be a validator, holding all other factors fixed, i.e. personal preference, irrationality, etc. Therefore, I would recommend Cosmos governance board to incentivize validators more by increasing the rewards, lowering the risks, etc.

Takeaways

It is of great necessity to build a governance system with democracy, flexibility, efficiency and economics of scale, thereby guaranteeing the decentralized network to be in good operation and management. As for CertiK's unique dual-pass governance model with three main participants which are stake delegators, validator operators and security certifiers, it is essential to incentivize each role similarly. Also, there are tradeoffs between efficiency and decentralization. My suggestion is to set clear and smart requirements and responsibilities for each role, letting them perform their duties respectively but can restrain each other at the same time.

3. Tendermint vs Casper

Pros

Cosmos Network uses Tendermint, which strictly prioritizes consistency and safety over availability and liveness. It guarantees that blockchain never forks assuming less than 1/3 of the validators are

Byzantine. Moreover, when it comes to a new proposal, Tendermint improves efficiency and convenience to compress multi-round voting process into a single round.

Cons
Due to the requirement of finality at time of block creation, block times should be short, which limits the number of validators that Tendermint can accommodate.

Takeaways
A broad overview of consensus algorithms should be addressed before we jump into the takeaway.

In general, there are varying ways to implement PoS algorithms, but the two main tenets in PoS design are chain-based PoS and BFT-based PoS. Tendermint is a BFT-based PoS, Casper the Friendly Ghost (CTFG) is a chain-based PoS, Casper the Friendly Finality Gadget (CFFG) is a hybrid of PoW and PoS implementation. Chain-based PoS prioritizes availability, liveness over consistency and safety while BFT-based PoS chooses the opposite.

As we've already discussed pros and cons of Tendermint, here we will briefly talk about CTFG and CFFG. Currently, CFFG still uses Nakamoto PoW consensus where miners create the blocks; however, Casper's PoS takes control and has its validators vote on blocks trailing the PoW miners. Also, CFFG has 20 minutes of finality. Fifty blocks are finalized every time to prevent brute force PoW mining attacks. Moreover, CFFG has a 51% threshold of attack resistance. With regard to PoS-designed CTFG with cartel resistance as its distinguished feature, it explicitly combats oligopolistic attackers so that no colluding set of validators can overtake the protocol.

There are tradeoffs between consistency, safety and availability, liveness. At present, CertiK uses Tendermint; in the future, applying which consensus algorithm is subject to the CertiK's underlying economic conditions, own risk preference, overall block chain environment, etc. Generally, there are some recommendations which can help PoS consensus algorithm arrive an optimal point and adopt the best practice.

First, it is suggested to leverage more advanced cryptography in order to make the signatures on the block headers smaller. If CertiK wants to join the idea of creating the Internet of Blockchains, moving light client proofs from one blockchain to another is the core. It would be hugely advantageous to use more advanced cryptography to decrease the size of the block headers by a factor of thirty or more. Tendermint block headers now are little less than 4 KB with 100 validators; they're full of validator signatures. Possibly we can make the 100 signatures go from 3.2 KB to 64 bytes.

Second, peer-to-peer layer can be optimized so that we can significantly decrease the amount of peer-to-peer traffic which is needed to finalize a block. This can not only compress the amount of data that goes into the block header, but decrease the amount of data sent to each peer. This will allow Tendermint to accommodate a larger set of validators than the current amount.

A Separate Topic of Network Security to Add On…

The major breakthrough of Cosmos Network is the goal to create the Internet of Blockchains by introducing Tendermint, IBC, Cosmos Hub, etc. to realize scalability, usability and interoperability of blockchain network.

However, the idea of creating the Internet of Blockchains will require a higher level of network security. The interoperability of blockchains makes easier to attack the network. Besides, any programming languages can be used in the Cosmos network may increase the potential risk of network security. For instance, C has higher vulnerabilities than Java, Python and Ruby. Furthermore, since all inter-zone token transfers go through the Cosmos Hub, the security of transactions via Cosmos Hub also faces challenges.

Security is indispensably paramount to blockchain network. CertiK Chain, as the network of CertiK, aims to provide truly unrivaled end-to-end security, from the long-term standpoint of an enterprise. Apart from its current mechanisms of achieving this goal, i.e. security verified cryptographic certificates, formal verified CertiK Virtual Machine (CVM), verified compiler assurance, functional programming language DeepSEA, the world's first and only fully verified hypervisor CertiKOS, a few takeaways can be learned from Cosmos Network as summarized here.

- Multi-token model
- Atom inflation method
- Network Tax collected to use for security issue
- Hardware Security Modules
- Physical security in data centers
- Set up a resilient sentry node
- Securely generating keys
- Security Audits…

In the end,

The development of blockchain industry is supposed to be consistent with economic essence. Sensible solutions are supposed to comply with principles of game theory, Nash Equilibrium, financial economics theory, behavioral economics, etc. Sometimes, we can also utilize econometric models to validate our thoughts. I hope this article helps.

References

Overall
1. https://blog.cosmos.network/economics-of-proof-of-stake-bridging-the-economic-system-of-old-into-the-new-age-of-blockchains-3f17824e91db
2. https://cosmos.network/intro
3. https://cosmos.network/resources/whitepaper
4. https://medium.com/@tokengazer/tokengazer-crypto-review-in-depth-analysis-of-cosmos-7caf4c4958cc

Part I
Tendermint
5. https://tendermint.com/static/docs/tendermint.pdf
6. https://tendermint.com/core/
7. https://docs.tendermint.com/master/
8. https://docs.tendermint.com/master/introduction/what-is-tendermint.html
9. https://www.youtube.com/watch?v=pBBdOD63K38
10. https://github.com/tendermint/tendermint

Cosmos SDK
11. https://github.com/cosmos/cosmos-sdk/

Inter-Blockchain Communication & Peg Zone & Hard Spoon
12. https://github.com/cosmos/ics/tree/master/ibc
13. https://cosmos.network/ibc
14. https://www.youtube.com/watch?v=z23itFlVCBc
15. https://blog.cosmos.network/the-internet-of-blockchains-how-cosmos-does-interoperability-starting-with-the-ethereum-peg-zone-8744d4d2bc3f
16. https://blog.cosmos.network/introducing-the-hard-spoon-4a9288d3f0df
17. https://cryptovest.com/education/the-hard-spoon-concept-explained/

Cosmos Hub & Zones
18. https://hub.cosmos.network/master/hub-overview/overview.html
19. https://github.com/cosmos/cosmos/blob/master/FAQ.md

Atoms & Photons & Whitelisting Tokens

Validators & Delegators
20. https://www.mangoresearch.co/blockchain-consensus-vs-validation/
21. https://github.com/cosmos/cosmos/blob/master/VALIDATORS_FAQ.md

Part II
Game Theory Analysis of Tendermint
22. https://mp.weixin.qq.com/s/maHfy2Wn5ImCuSMxRStNqQ
23. https://www.binance.vision/blockchain/byzantine-fault-tolerance-explained

Utility Analysis of Cosmos Tokens
24. https://github.com/cosmos/cosmos/blob/master/Cosmos_Token_Model.pdf

Incentive Analysis of Atom Holders
25. https://blog.chorus.one/pos-ecosystem-101/
26. https://blog.chorus.one/proof-of-stake-ecosystem-102/

27. https://blog.chorus.one/cosmos-staking-reward-primer-reward-calculator/

Part III
Multi-Token Model

Governance
28. https://figment.network/resources/cosmos-governance-february-update/#discussions
29. https://medium.com/certik-foundation/certik-chain-governance-overview-ce0eb8d0597a

Tendermint vs Casper
30. https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae

Network Security
31. https://medium.com/certik-foundation/certik-chain-governance-overview-ce0eb8d0597a
32. https://medium.com/certik-foundation/certik-chain-deepseas-native-chain-6cd9cc727c3b