The Governance of Cosmos Interchain Security

Darcy W.E. Allen[1], Chris Berg[2] and Sinclair Davidson[3]
RMIT Blockchain Innovation Hub

Supported by the ATOM Accelerator DAO

This version November 2023

Abstract: Interchain security (ICS) allows the Cosmos Hub to provide security to other blockchains ('consumer chains') and represents a significant revenue model for the Cosmos Hub. This paper investigates the economic and governance aspects of these ICS agreements with a focus on ensuring that the agreements are value adding and robust. The paper identifies potential risks such as vertical integration, challenges in adapting to incomplete contracts, and opportunism in asset-specific investments. It proposes recommendations to enhance the sustainability of ICS relationships, including the establishment of individual governance bodies for each ICS agreement, strategies to manage foreign exchange risks, and a decision tree for the Cosmos Hub to assess new consumer chains. A draft template for consumer chain onboarding is also presented, detailing essential elements like governance, payment terms, and exit clauses. This paper aims to offer actionable insights for improving the governance structures in ICS agreements, thereby fostering robust and enduring interchain security dynamics.

Keywords: Interchain Security, Shared Security, Cosmos Hub, Institutional Cryptoeconomics, ATOM, Tokenomics

1. Introduction

The Cosmos Hub is a unique blockchain in the global cryptoeconomy.[4] As the largest chain in the ecosystem which has grown up around it, it can leverage its dominant stake weight to create a long term sustainable business model for the benefit of token holders and the ecosystem. This paper contributes to the development of that business model. The aim of this paper is to examine and provide recommendations on replicated security in interchain security from an institutional economics perspective, helping to ensure that ICS agreements are sustainable, robust and mutually beneficial. Our view is that fundamentally the relationship between the Cosmos Hub and any given consumer chain is a governance relationship. Like all economic relationships, ICS agreements will suffer from potential governance hazards, particularly as the Cosmos Hub and the consumer chains evolve. We aim to identify some of these hazards and

[1] Blockchain Innovation Hub, RMIT University. email: darcy.allen@rmit.edu.au
[2] RMIT Digital3 and Blockchain Innovation Hub, RMIT University
[3] Blockchain Innovation Hub, RMIT University
[4] This paper draws on some of our Cosmos Hub Governance Forum posts. See: https://forum.cosmos.network/t/discussion-principles-for-onboarding-consumer-chains-into-the-aez/11571 and https://forum.cosmos.network/t/discussion-governance-of-ics-rmit-aadao-project-update/11498

provide recommendations about how they might be mitigated. We also provide recommendations and principles upon which the Cosmos Hub community might consider onboarding a new consumer chain. We proceed as follows.

- **Section 2** introduces interchain security and explores its evolution, including future models of customizability.
- **Section 3** frames ICS as a make or buy decision. Shared security models are fundamentally a decision by a consumer chain to buy security rather than make it in-house. We explore some of the benefits of shared security markets for both the Cosmos Hub and consumer chains.
- **Section 4** analyses the risks in ICS shared security. We look back to historical security provision before identifying risks in ICS agreements stemming from incomplete contracts and bounded rationality. There are risks of opportunism both before onboarding (e.g. asymmetric information) and after onboarding as those relationships evolve (e.g. the hold up problem).
- **Section 5** lays out three solutions to these contracting problems: (1) vertical integration; (2) joint-production; and (3) long-term contracts. The former two options are not conducive to the values of Cosmos, and so risks must be managed as long term contracts. This motivates our discussion of how the risks of long-term ICS contracts could be mitigated.
- **Section 6** turns to a crucial but underappreciated question: what is the purpose of ICS agreements from the perspective of the Cosmos Hub? We identify two categories: (1) that the Cosmos Hub is a venture investor in a consumer chain, seeking upside; or (2) that the Cosmos Hub is an infrastructure provider, seeking revenue. The way that a given consumer chain is viewed impacts who bears the foreign exchange risk from the relationship.
- **Section 7** provides some specific recommendations and findings from the analysis, including (1) the establishment of an agreement-level ICS governance body; (2) a decision tree for onboarding from the perspective of the Cosmos Hub; and (3) an onboarding template for consumer chains (including details such as compensation structure and governance processes).
- **Section 8** concludes.

2. The evolution of interchain security

The Cosmos Hub has been described as a port city.[5] It connects other sovereign blockchains to create an interchain economy, enabling a process of emergent ordering rather than top-down planning. To achieve this port city status, the evolution of the Cosmos Hub infrastructure "secures trade, promotes exchange, brings people and resources and opportunities together to create their own self-determined, self-governed communities."[6]

The 2023 launch of interchain security (ICS) continues this path of the Cosmos Hub becoming a port city.[7] ICS enables "a ground-up framework for … projects to securely deploy within the

[5] See Buchman, Ethan and Hart, Sam "The Cosmos Hub is a Port City" https://blog.cosmos.network/the-cosmos-hub-is-a-port-city-5b7f2d28debf
[6] Buchman, Ethan and Hart, Sam "The Cosmos Hub is a Port City" https://blog.cosmos.network/the-cosmos-hub-is-a-port-city-5b7f2d28debf
[7] See WillB (2023) "Enabling the ATOM Port City", Cosmos Hub Forum, 27 October https://forum.cosmos.network/t/enabling-the-atom-port-city/11909

Cosmos Hub's 'ATOM economic zone' by leveraging the Hub's validator set."[8] ICS is part of a broader family of efforts to facilitate shared security in blockchains. These shared security models enable markets for security across blockchain boundaries (e.g. between a consumer and producer chain, between different layers of a blockchain stack). While the focus of this paper is on shared security in Cosmos, there are broader implications of these governance relationships the build-out of shared security models elsewhere.

The first iteration of shared security in Cosmos is replicated security. In replicated security, the producer chain (the Cosmos Hub) enables its validator network to validate transactions and secure the network of another chain (the consumer chain). At the time of writing consumer chains include Stride and Neutron. The Cosmos Hub validators essentially replicate their security services onto the consumer chain, ensuring consistency and integrity of data, and leveraging the economic weight of ATOM. The consumer chain, in turn, compensates the Cosmos Hub for this security service (e.g. with a revenue share). This compensation ensures "that delegators on the provider chain are compensated for infrastructure maintenance and slashing risk resulting from validating the consumer chain."[9]

Replicated security is only the first iteration of ICS and it will evolve over time. Future iterations of shared security will provide more customised and complex relationships between producer chain(s), consumer chains, and delegators, for instance:[10]

- **Mesh security** might enable ATOM delegators on the Cosmos Hub to delegate their ATOM stake to validators in a consumer chain.[11] This shifts some decision making from Hub validators to ATOM token holders, allowing chains to "increase each other's security bidirectionally".[12]
- **Opt-in security** might enable Cosmos Hub validators to decide whether they would like to provide validation services to a given consumer chain. Rather than replicating the entire validator set this model enables greater optionality for validators (particularly for large validators).
- **Layered security** opens up the possibility for multiple producer chains, with consumer chains combining security from different sources.[13]

Each of these future evolutions trade-off in characteristics such as complexity, robustness and customizability. Much of the ways that these trade-offs manifest will be revealed through application in practice.

---

[8] 0xspaydh (2023) 'Replicated Security and Why it Matters for Cosmos', *HackerNoon*, 25 April, https://hackernoon.com/replicated-security-and-why-it-matters-for-cosmos

[9] Tremback, Jehan (2022) 'An Overview of Interchain Security v1', *Informal Systems Blog*, 2 February, https://informal.systems/blog/interchain-security-v1

[10] For some descriptions of these models see Cosmos Christina (2023) 'Interchain Security Begins a New Era for Cosmos' 17 May, *Cosmos Network Blog* https://blog.cosmos.network/interchain-security-begins-a-new-era-for-cosmos-a2dc3c0be63

[11] For a comparison of replication and mesh security see Jehan Tremback, Marius Poke, Juan Beccuti (2022), ' Replicated vs. Mesh Security' Informal Systems Blog https://informal.systems/blog/replicated-vs-mesh-security

[12] Cosmos Hub (2023) 'Comparing Replicated, Opt-in, and Mesh Security' *The Interchain Foundation Medium*, 23 May, https://medium.com/the-interchain-foundation/comparing-replicated-opt-in-and-mesh-security-a24d67e04b81

[13] For a brief description of layered security see Billy Rennekamp (2021) 'Interchain Security is Coming to the Cosmos Hub', Interchain Ecosystem Blog, 1 September https://blog.cosmos.network/interchain-security-is-coming-to-the-cosmos-hub-f144c45fb035

Even in replicated security, each relationship in ICS is unique because the consumer chains are diverse, leading to diverse ICS contracts. Consumer chains are sovereign, have their own business model and potential, and often their own community. This heterogeneity is and will continue to be reflected in ICS contracts. Each will propose different shared security arrangements to the Cosmos Hub. For instance:

- Neutron launched on replicated security, providing 25% of their transaction fees and MEV revenue.[14]
- Stride was an established blockchain that joined the Atom Economic Zone (AEZ) through replicated security, proposing to provide 15% of liquid staking rewards, inflationary rewards, MEV revenue and transaction fees, as well as asking for a significant allocation of ATOM from the community pool as protocol owned liquidity.[15]

These both represent different revenue sharing models. We anticipate more complex compensation ICS relationships as the AEZ builds out, including technical capabilities that expand the design space of possible relationships.

Shared security models provide tangible benefits for both the producer and consumer chain. Smaller chains receive lower-cost access to high quality security from the Cosmos Hub. Shared security "lowers the barrier to launching secure sovereign decentralized chains".[16] Spinning up a decentralised validator set "has been a hurdle for many projects who would otherwise benefit from running on a Cosmos Chain."[17] There are also associated opportunity costs of dedicating resources towards making your own security, including "a distraction from building a community of engaged users" and how this can "complicate a project's tokenomics".[18] The provision of shared security also benefits the Cosmos hub, not least by generating new revenue streams through providing services and leveraging the economic weight and expertise of the existing validator set.

3. Shared security and the 'make or buy' decision

In this seminal work, *The Nature of the Firm*, economist and Nobel laureate Ronald Coase asked why firms exist. His answer was deceptively simple: in some circumstances, it is more efficient to conduct transactions within an organised firm than it is on an open market.[19] Organising in a firm through a hierarchy can suppress some of the costs associated with engaging in trade over a market. But firms too come with costs that are not in markets, thereby creating a boundary between organisation in firms and in markets. There are different costs of organising production within a firm rather than over a market, and these costs create a decision: make or buy?[20]

[14] For the Neutron proposal see https://forum.cosmos.network/t/proposal-792-accepted-launch-neutron-on-replicated-security/10230
[15] For the Stride proposal see https://forum.cosmos.network/t/proposal-794-vote-onchain-stride-to-join-atom-economic-zone-and-adopt-ics/10418
[16] See https://blog.cosmos.network/interchain-security-begins-a-new-era-for-cosmos-a2dc3c0be63
[17] See Jehan Tremback (2022) 'Building With Interchain Security' Informal Systems blog, 9 May, https://informal.systems/blog/building-with-interchain-security
[18] See Jehan Tremback (2022) 'Building With Interchain Security' Informal Systems blog, 9 May, https://informal.systems/blog/building-with-interchain-security
[19] Coase, R. (1937) 'The Nature of the Firm', *Economica* 4(16): 386-405
[20] Klein, P. G. (2005). The make-or-buy decisions: Lessons from empirical studies. *Handbook of New Institutional Economics*, 435-464.

Either making or buying services faces transaction or other coordination costs. Buying through market-based transactions has costs involved in searching, negotiating and enforcing contracts, as well as hazards. Making in-house within a firm has costs of management, coordination and shirking. Understanding such transaction costs helps us to navigate the make or buy decision. Should you make a product or service in-house, or should they buy the product or service over a market? Which approach more effectively economises on the costs of economic activity?[21]

The entrepreneurial process of building blockchain applications generates many 'make or buy' decisions. For instance, should a blockchain project make a new custom wallet, or integrate into an existing wallet? Should a project develop a native stablecoin, or utilise an existing stablecoin with its established base of users and liquidity? As the choices for external blockchain infrastructure toolkits grows — including increasing interoperability across those tools — we will see more decisions to buy.[22] That is, more market-based building up of business models.

A make or buy decision also exists regarding security. Should a blockchain develop security by spinning up and maintaining security infrastructure, or purchase security services from another producer? There are clearly costs and benefits to each. The success of shared security models, including ICS, are premised on the idea that some blockchains will be willing to buy security rather than make it. As we will see throughout this paper, there are various ways, such as through more effective governance, that we can reduce the transaction costs of buying security (rather than making it).

One major driver of the decision to make or buy security are the transaction costs of the alternatives. Nobel Laureate Oliver Williamson has described in detail how structures of transaction costs (e.g. asset specificity, uncertainty) change the effective type of economic organisation (e.g. markets or hierarchies).[23] Making security in-house might reduce transaction costs by providing a level of control, with greater override over its security practices and ability to tailor them to its specific needs rapidly (e.g. in response to an incident). This in-house approach, and the control it offers, might also more closely align with the value of sovereignty. While a blockchain might not have direct control over its validators, it can implement rules to shift incentives within that validator set.

There are several clear benefits for the consumer and producer chain in shared security. These are the gains from trade.[24] Consumer chains may receive enhanced security, but without bearing the direct costs and complexities of establishing and maintaining their security infrastructure. The producer chain can leverage its shared security infrastructure, namely the validator set, to diversify their customer base and to receive new revenue streams. Following in the notion of Hub minimalism, the Cosmos Hub could, for instance, spin off business models and infrastructure as consumer chains, supporting them through shared security provision.[25]

---

[21] Besanko, D., Dranove, D., Shanley, M., & Schaefer, S. (2009). *Economics of strategy*. John Wiley & Sons.
[22] On toolkits in a web3 context see Allen, Darcy. W. E, & Potts, Jason. (2023). 'Web3 toolkits: A user innovation theory of crypto development'. *Journal of Open Innovation: Technology, Market, and Complexity*, 9(2), 100050.
[23] Williamson, Oliver (1985) *The Economic Institutions of Capitalism*. Free Press: New York.
[24] By engaging in trade, individuals leverage their unique skills and resources to specialise in areas where they hold a comparative edge, optimising their productivity and earning potential while reducing the cost of acquiring assets or resources that they need. The gains from trade have been emphasised in economics since Adam Smith wrote the *Wealth of Nations* in 1776.
[25] In Section 6 we discuss the distinction between a venture and an infrastructure relationship.

Our focus here is on costs. Making security has both direct and indirect costs. The direct costs of making security include recruitment, salaries, and ongoing maintenance of validators. In the decentralised context of Cosmos, this relationship is complex, and includes the inflation costs and fees to validators themselves. There are hardware costs involved, most of which are borne by the validators. While many of these costs are borne by the validator set themselves, there are significant coordination costs in achieving this. Perhaps more abstractly are the costs of

	Make Security	**Buy Security**
Benefits	● Sovereignty for consumer chain ● Control over security (e.g. customizability to change security parameters, such as consensus processes) ● Avoids some costs of buying security from a producer chain ● Producer chain validators do not need to bear the costs of ICS (e.g. can focus on validating Cosmos)	● Gains from trade for both the consumer and producer chain (e.g. revenues for cosmos Hub, higher quality security for consumer chain) ● Enhanced security with the economic weight of the Hub ● Avoid the direct costs of establishing and maintaining a validator set ● Makes the establishment of more blockchains possible by lowering barriers to entry
Costs	● Consumer chain bears direct costs of establishing and maintaining a validator set (including costs of maintenance and hardware), coordination costs of hundreds of dispersed actors, costs of building expertise in security provision ● Potentially greater attack vectors for consumer chain due to lack of economic weight ● Opportunity costs from diverting resources towards producing securit ● Producer chain does not leverage its security expertise	● Both parties face basic governance and transaction costs including searching, negotiating and enforcing an ICS agreement ● Asset specific investments that are not easily recoverable if the relationship fails ● Potential risk of opportunistic behaviour (e.g. hold up by the producer chain following asset specific investments) ● Cosmos Hub validators bear fixed costs of integrating consumer chain

specificity (of investing in asset special hardware and knowledge). When transactions involve high asset specificity, making security can mitigate potential hazards associated with opportunistic behaviour.[26]

The indirect costs of making security are less tangible but still significant. There are opportunity costs, for instance, of the potential diversion of resources and focus away from the core operations and value proposition of the project.[27] There could also be costs related to risks and liabilities if a security breach occurs, which could harm the network's reputation and lead to the loss of trust among its users.

[26] Some of these asset specific investments in an open blockchain context, however, might be more complex than in a traditional environment. For instance, 'making' your security in house doesn't necessarily (or even desirably) require owning validators.

[27] Opportunity cost is usually defined as being the value of the next best alternative that must be foregone as a result of choosing one option over another.

Many of these direct and indirect costs of making security are exacerbated for smaller blockchains with fewer resources and expertise. This has parallels to well-understood challenges of how excessive regulatory barriers impose a greater burden on smaller organisations (partly because they lack the expertise and resources to deal with them).[28] Furthermore, until recently the blockchains that did not have the resources to pay for the costs described above would simply not launch. We cannot see those projects that have decided not to launch because of costs — those that are effectively priced out of joining the cryptoeconomy. But now, through shared security, those blockchains have the option to buy security through ICS.

The focus of this paper is on the ways that we can reduce the costs of buying security. Where the option to buy security is available, generally chains will decide to buy security where the costs of buying security are lower than the costs of producing security in-house. These costs manifest in different transaction costs including those of incomplete contracts, asymmetric information and various types of opportunism (see Section 4 below). For instance, buying security rather than making it raises additional complications of incomplete contracts because not all future contingencies can be contractually specified. In choosing a producer chain, the consumer chain may make asset specific investments that are not easily recoverable if, for instance, that producer chain does not effectively provide the security suggested they have specified. On the other hand, these assist specific investments of the producer chain might use their advantageous position to renegotiate ICS agreements. Our ability to reduce these costs through governance will expand the potential scope of shared security.

4. Risks in shared security and ICS agreements

4.1. Historical shared security

Shared security models are not new. Historically, security providers have leveraged their power into a position of control — both in political security provision and corporate security provision.[29]

Political security provision has manifested in many undesirable ways. In medieval Europe, feudal lords provided security to peasants in exchange for labour and loyalty. This arrangement also bound peasants to the land and gave lords significant power over their lives. European powers, under the guise of bringing ‘civilisation’ and ‘security’ to colonised regions, often exerted control over indigenous populations, extracting resources and suppressing local cultures. In some authoritarian regimes, security forces, which ostensibly exist to protect the populace, are employed more for state surveillance and suppression of dissent.

In private markets, corporate security provision, those risks manifest in distinct undesirable outcomes. One organisation providing security for another can lead to either vertical integration[30] or diversified conglomerates.[31] In the former one company takes control of multiple parts of its production process. A car manufacturer, for instance, might own the steel plant that

[28] Peltzman, S. (1976). Toward a more general theory of regulation. *The Journal of Law and Economics*, 19(2), 211-240.
[29] Barzel, Y. (2002). *A theory of the state: economic rights, legal rights, and the scope of the state*. Cambridge University Press.
[30] Klein, B., Crawford, R. G., & Alchian, A. A. (1978). Vertical integration, appropriable rents, and the competitive contracting process. *The Journal of Law and Economics*, 21(2), 297-326.
[31] Langlois, R. N. (2023). *The Corporation and the Twentieth Century: The History of American Business Enterprise*. Princeton University Press.

produces metal for its cars, ensuring control from raw material extraction to the final product.[32] Once a firm has secured its supply chain and information flow through vertical integration, it can dictate terms downstream and upstream. This control can lead to reduced competition and the creation of barriers to entry, further entrenching the firm's dominant position. In the latter, diversified conglomerates are corporations that own a diverse range of businesses, often in unrelated fields. With a presence in multiple sectors, conglomerates can exert influence over a broad spectrum of the market. Their sheer size and reach give them significant bargaining power over suppliers, distributors, and even regulatory bodies. The capacity for these conglomerates to cross-subsidise also allows them to undercut competitors in strategic areas, reinforcing their control.

At first glance the strategic consolidated market power of vertical integration and diversified conglomerates seems good for shareholders. Why wouldn't you want to control more of your production processes and suppliers? But these structures also often generate inefficiencies that are bad for shareholders. For instance, these structures suppress innovation by reducing competition. Firms get bogged down in bureaucracy and lack the ability to respond to changes.[33] Managing disparate business units in a conglomerate is complex and can blur strategic focus. Expertise can be diluted across the organisation, leading to suboptimal allocation of capital. As these entities grow, they risk becoming too unwieldy, making internal communication challenging, and often end up supporting underperforming units at the expense of those with higher potential, ultimately undermining overall corporate profitability and value.[34]

These historical outcomes from shared security — feudalism, colonialism, vertical integration, diversified conglomerates — sit in tension with many of the values of decentralised infrastructure communities such as Cosmos. What we have described here doesn't square with sovereign interoperability. Unless the Cosmos Hub effectively mitigates these risks of centralisation of power, there are significant risks to the viability of the decentralised ecosystem. For instance, it is necessary to ensure that the role of the Cosmos Hub as security provider does not gain undue influence over a consumer chain's operation. Indeed, just as feudal lords or diversified conglomerates exercise their power through the provision of security services, so too could the Cosmos Hub. For instance, the Hub could dictate terms or extract disproportionate fees.

While it is worthwhile keeping these broad threats in mind, we now more specifically examine the risks inherent in an ICS relationship. The aim of this analysis is to implement mechanisms that preserve the autonomy and sovereignty of both chains, enabling them to benefit from the creation of the AEZ.

4.2. Contracting hazards in ICS

4.2.1. Bounded rationality and the world

The governance relationship between the parties to an ICS agreement are fundamentally incomplete. A producer-consumer chain ICS relationship is not merely technical — it is a long-

[32] Coase, R. H. (2000). The acquisition of Fisher Body by general motors. *The Journal of Law and Economics*, 43(1), 15-32.
[33] Shleifer, A., & Vishny, R. W. (1991). Takeovers in the'60s and the'80s: Evidence and implications. *Strategic Management Journal*, 12(S2), 51-59.
[34] Berger, P. G., & Ofek, E. (1995). Diversification's effect on firm value. *Journal of Financial Economics*, 37(1), 39-65.

term economic relationship. While this relationship might begin in a mutually beneficial way, as the chains evolve, and the environment around them shifts, these relationships will face hazards. Many of these hazards are not new and are well-understood in research detailing contract design in industrial organisation.[35] Contracts are incomplete for many reasons, fundamentally stemming from our cognitive limitations (bounded rationality) and unforeseen changes.[36]

Challenge	**Implications for contracting**
Cognitive limitations (bounded rationality)	Humans cannot possibly process all possible scenarios or outcomes. We have a lack of foresight and inability to cognitively process all possible information about the agreement, and then detail that in a contract.
The world is unpredictable	Unforeseen events or consequences happen that are beyond the control of the parties. For instance, there might be unexpected changes in hardware costs for validation, or the establishment of a major competitor to the consumer chain or the Cosmos Hub.

Even with the best intentions, as humans we have intrinsic cognitive limitations, often referred to as bounded rationality.[37] Our capacity to store, process, and communicate information is finite. This means that, no matter how thorough a contract is, it's improbable for it to encapsulate every possible scenario or outcome, simply due to our inability to foresee or articulate all potential variables.[38] Even if we could plausibly predict every possible scenario or outcome, the reality is that it costs time and money to draft contracts.

Drafting a contract that accounts for every conceivable scenario is not only cognitively challenging but also time-consuming and expensive. The effort and resources required for exhaustive contingency planning often outweigh the perceived benefits, leading parties to accept a certain level of incompleteness as a trade-off. Contracting costs also arise in terms of monitoring costs (e.g. ensuring the counterparty delivers) and enforcement costs (e.g. enforcing the contractual terms).

Underpinning these challenges is the fundamental reality that the world changes. The unpredictable nature of the world means that unforeseen events or consequences can arise, which weren't considered during the drafting of the contract. These 'black swan' events can leave significant gaps in even the most comprehensive agreements.

[35] Milgrom, P. & Roberts, J. (1992). *Economics, organization and management*. Englewood Cliffs, NJ: Prentice-Hall.
[36] Scott, R. E., & Triantis, G. G. (2005). Incomplete contracts and the theory of contract design. *Case Western Reserve Law Review* 56, 187.
[37] Simon, H. A. (1997). *Models of bounded rationality: Empirically grounded economic reason*. MIT press.
[38] Gigerenzer, G. (1997). Bounded rationality: Models of fast and frugal inference. *Swiss Journal of Economics and Statistics*, 133(2/2), 201-218.

4.2.2. Opportunism

Both examples above still assume that both producer and consumer chains will act in good faith. But of course, either the producer or consumer chain could act opportunistically. Opportunism is a multifaceted concept that reflects self-interested behaviour characterised by cunning or guile.[39] At its core, opportunistic actions can manifest in overtly malicious ways, such as lying, stealing, or cheating. However, they can also take more subtle forms, like obfuscation or nuanced deceit, which might not be immediately evident but can have long-term detrimental effects on contractual relationships.[40] There are several ways that opportunism could manifest in ICS agreements. Below we outline broadly how some forms of opportunism could emerge both before an ICS agreement is struck (*ex ante* opportunism) and afterwards (*ex post* opportunism), and some potential solutions. First we summarise this in a table.

Type of opportunism	**Manifestation**	**Examples**	**Solutions**
Ex ante opportunism			
Asymmetric information	Either party possessing more or better information than the other	Consumer chain withholding information about potential product roadmap Producer chain withholding information about consumer chain competitors	Signalling (e.g., showcasing existing business model), Screening (e.g., rigorous proposal review during onboarding)
Adverse selection	One party making decisions that adversely impact the other	Consumer chain inflating its token or changing its fee structure	Signalling, Screening, Clear disclosure requirements, Transparency in discussions
Ex post opportunism			
Asset Specificity and the Hold-up Problem	Parties locked into suboptimal agreements due to relationship-specific investments	Producer chain leverages the locked-in position of the consumer chain to extract existing rents	Comprehensive contractual safeguards, predefined exit/repricing terms, Competitive options
Performance Management	Ambiguous or challenging	Exaggerating growth, under-reporting	Clear performance metrics, transparent

[39] Williamson, O. E. (1979). Transaction-cost economics: the governance of contractual relations. *The Journal of Law and Economics*, 22(2), 233-261.
[40] Williamson, O. E. (1993). Opportunism and its critics. *Managerial and Decision Economics*, 97-107.

Challenges	performance measurement	challenges	reporting
Maladaptation Costs	Failure to adapt to changing circumstances optimally	ICS agreement prevents either or both consumer and producer chain from adopting new innovation	Discrete mechanism for renegotiation

4.2.2.1. Asymmetric information and adverse selection (ex ante opportunism)

Opportunistic behaviour can happen before an agreement is struck — that is, before a consumer chain is onboarded into the AEZ. There are various ways that this *ex ante* opportunism can manifest. Either party could possess more or better information than the other party — known as **asymmetric information**.[41] Either party could leverage asymmetric information (where they have more or better information than the other party) in contract formation or renegotiation. A consumer chain might have better information about their potential product roadmap, or the Cosmos hub might have better information about competing projects to the consumer chain. This private information might be withheld to create a more favourable contracting arrangement.

More examples are illustrative here. Imagine a consumer chain is paying the Cosmos Hub in their own native token. That consumer chain could make opportunistic decisions around that asset (e.g. inflating the token) or their ecosystem (e.g. changing their fee structure). The residual bearers of those costs may be the validators and the Cosmos Hub, despite the fact they are not involved in the governance on the consumer chain.

Traditionally, *ex ante* opportunism is solved through either signalling or screening.

- **Signalling.** One party conveying information (a signal) about its type or quality to counteract information asymmetry. For instance, a job applicant might signal their competence by showcasing their educational qualifications. In ICS, a consumer chain might demonstrate their existing business model, or they might make some credible commitment, such as an airdrop or allocation to the Cosmos Hub token holders or validators.
- **Screening.** Here, the less informed party can gather more information about the other. In a traditional environment, screening could involve an employer screening potential employees through rigorous interview processes. In ICS, screening involves a rigorous process of proposals and discussion on the Cosmos Hub forum and elsewhere. That is, screening happens through the onboarding process. The onboarding template presented later in this paper facilitates this screening process.

4.2.2.2. Asset specificity and the hold up problem

Ex post opportunism arises after a consumer chain is onboarded into ICS. The most obvious form of *ex post* opportunism is backtracking or breaking previously agreed upon terms. This type

[41] Hillier, B. (1997). *The economics of asymmetric information*. Bloomsbury Publishing.

of opportunism gives rise to distrust and, depending on the circumstances, can manifest in inefficiencies arising from either underinvestment or overinvestment as parties deliberately invest either less than required or disproportionately more, aiming to shift costs or benefits.

Over the course of a contractual relationship, there can be instances where parties fail to adapt to changing circumstances optimally. Opportunistic individuals or entities can capitalise on these maladaptations[42], deriving undue benefits or shirking responsibilities. Maladaptation costs arise because parties can get locked into suboptimal agreements as those changes occur.

There can also be challenges of performance management. Contracts often have stipulations regarding performance metrics or deliverables. However, when the measurement of these performances is ambiguous or challenging, it opens the door for opportunistic behaviour. Parties might exaggerate achievements, under-report inefficiencies, or manipulate data to appear in a more favourable light.

One of the major ways that *ex post* opportunism manifests is in the **hold-up problem**.[43] Hold-up becomes especially problematic once 'fundamental transformation' has occurred.[44] This is a term coined by Oliver Williamson and represents a pivotal shift from a general, competitive market setting to a unique, bilateral relationship between contracting parties.[45] Initially, parties might engage under market-based conditions, where multiple sellers and buyers exist. However, as they invest and commit resources specific to the relationship, they transition from this open market competition to a situation of mutual dependence, characterised by the bilateral monopoly. Central to this transformation is the concept of asset specificity.[46] Asset specificity refers to the extent to which the value of an investment is contingent on its use within a particular context or transaction, making it inherently less versatile or transferable across alternative uses or by different users.

Where consumer and producer chains may have made relationship-specific investments to enter the AEZ — including the developer costs of integration — there is a risk of hold up. If an ICS agreement was to fail then those investments would be lost. There are several types of asset specificity, not only including the code itself (i.e. aligned with the Cosmos Hub), but also human asset specificity and the skills and expertise generated specifically for the ICS relationship. The greater the degree of asset specificity, the deeper the lock-in effect and the more pronounced the 'fundamental transformation', potentially leading to challenges in renegotiation, hold-up situations, and the need for more comprehensive contractual safeguards.

---

[42] Maladaptation costs refer to the economic and social expenses incurred when actions intended to adapt to changes — like those associated with technological shifts, or market dynamics — unintentionally exacerbate vulnerability or create new problems. See Aoki, M. (1983). Managerialism revisited in the light of bargaining-game theory. *International Journal of Industrial Organization*, 1(1), 1-21.

[43] The hold-up problem occurs when one party in a transaction exploits the transaction-specific investments made by another party, knowing that the invested party is vulnerable to such opportunism due to the sunk costs they cannot recoup. See Klein, B. (1998). The hold-up problem. *The New Palgrave Dictionary of Economics and the Law*, Peter Newman, ed., Macmillan Reference Limited.

[44] The fundamental transformation refers to the process by which a competitive market transaction evolves into a monopolistic relationship following an initial agreement, as the initial bid winner becomes uniquely valuable due to asset specificity, reducing the bargaining power of the other party for subsequent transactions.

[45] Williamson, O. E. (1985). *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*. New York: Free Press.

[46] Riordan, M. H., & Williamson, O. E. (1985). Asset specificity and economic organization. *International Journal of Industrial Organization*, 3(4), 365-378.

Hold up can also emerge due to rapid changes in the nature of the agreement itself. Consider the situation when a consumer chain is wildly successful, and their token price spikes significantly. The original ICS proposal pays a percentage of its transaction fees in a token native to the consumer chain. The Cosmos Hub has become reliant on the revenue, and the consumer chain is threatening to exit. How can the agreement be repriced so that the consumer chain does not exit and spin up a validator set, rather than renegotiate? What would the terms of exit be? Alternatively, imagine that a consumer chain fails, and their token price falls to near zero. Given potential ongoing costs for the validators and the Hub, how should the producer and consumer chain navigate this scenario. The producer chain might use the weakened position of the consumer chain to renegotiate, perhaps trying to vertically integrate.

5. Three solutions to contracting hazards

There are three major ways that the contracting hazards described above could be mitigated, with varying levels of desirability.[47]

5.1. Vertical integration

When one organisation brings under its umbrella multiple stages of the production process (including security provision) this is known as vertical integration. In the context of shared security, this is a form of centralisation, where both the producer chain and consumer chain are organised under some overarching administrative entity (even if that entity was ATOM token holders). There are of course benefits to this centralisation, including many of the benefits that Ronald Coase famously alluded to that we discussed in Section 3. This vertical integration approach, for instance, enables us to eliminate the need for a separate contract between the producer and consumer chain (as is the current approach in ICS). Subsequently this structure could mitigate some potential disputes (through authority) and overcome issues relating to contract incompleteness or the holdup problem.

Many challenges act as a friction against vertical integration. These include scope for monopolistic control over a consumer chain, compromising its integrity and trustworthiness. Furthermore, there are the broader impacts of reduced competition and potential inefficiencies that can arise from managing a sprawling, integrated enterprise. Centralisation could also introduce single points of failure, making the system more vulnerable to attacks or systemic failures.

But the major challenge with vertical integration is that it runs counter to one of the core Cosmos community values: sovereignty and decentralisation. Indeed, it is difficult to conceive what a consumer chain is as a standalone ecosystem if it has been vertically integrated, it is simply part of the Cosmos Hub. It certainly is not sovereign. For these reasons we do not consider vertical integration a plausible or desirable solution to the governance problems of ICS.

5.2. Joint Production

An alternative solution to shared security governance could be joint production. Here, the producer and consumer chain could come together to collaboratively produce goods or

[47] FitzRoy, F. R., Acs, Z. J., & Gerlowski, D. A. (1998). *Management and economics of organization*. Prentice Hall.

services. In this approach the producer and consumer chain would somehow jointly maintain and take responsibility for the security infrastructure.

There are many potential benefits of joint production, such as shared expertise across organisational boundaries. At least initially, joint production seems to align with the collaborative nature of the AEZ. But we argue that the nature of the relationship between a producer and consumer chain in shared security would create significant contracting hazards.

In a shared security context, joint production might lead to ambiguity in responsibility. The inherent complexities of managing a joint venture, such as aligning incentives, ensuring equal contributions, and addressing the horizon problem, can muddle accountability. Joint ventures also typically have slow decision-making processes, which doesn't align well with the dynamic nature of building decentralised ecosystems. The decentralised nature of blockchain demands a security approach that is both agile and devoid of central control points, making traditional mechanisms like vertical integration and joint production ill-suited for ensuring robust shared security in the blockchain landscape.

When responsibilities are shared in joint-production the risk of shirking increases (where one party reduces their effort), leading to conflicts. More tangibly for ICS, joint production can lead to a horizon problem where the investment horizons of the producer chain and the consumer chain does not align. For instance, one chain may be focused on short-term objectives (e.g. a consumer chain might seek to scale and exit), while the other has more long-term objectives (e.g. the Cosmos Hub might seek to grow the AEZ). Joint production also raises inalienability problems, where assets in an agreement can't easily be separated or transferred. This indivisibility of some of the underlying assets creates contracting hazards.

5.3. Long-term contracts

An alternative to either vertical integration or joint production is the development of long-term contracts. Here both the producer and consumer chain engage in an agreement across a long-term timeframe that is structured to offer both stability and predictability while maintaining independent governance of each party.

In a shared security context, there are many considerations to ensure the robustness, integrity, and mutual benefit of such long-term contracts.

The on-boarding process merits close attention. As consumer chains join the shared security framework, it's imperative to establish clear criteria, protocols, and checks to ensure that each participant aligns with the community's goals and standards. The initial expectation, based on current trends, is that many of these projects will likely be spin-offs from established entities like Cosmos or emerging start-ups. Given their nascent stages or derivative nature, these projects might come with unique challenges and requirements. These chains, being the recipients of the shared security, will have a significant impact on the community's dynamics.

The way that these long-term contracts are governed must also be considered. How can the long-term contracts be maintained over time to ensure the contract remains relevant and robust in the face of evolving threats? While in the short term some of this governance will occur in ICS-level governance bodies (see Section 8), there is also the potential for this governance to move towards ICS-specific DAOs. In the section below we turn to a critical dimension of long-term ICS

contracts, the exchange rate risk problem, which draws attention to the fundamental purpose of these agreements for the Hub as either venture relationships or infrastructure relationships.

6. The exchange rate risk problem

6.1. Who bears the exchange rate risk?

A core problem in the design of sustainable long-term ICS agreements is how payments for ICS should be denominated. Where consumer chains have their own native tokens, payments could be accepted in:

- native token of consumer chains
- ATOM
- a generally accepted medium of exchange in the cryptoeconomy, such as bridged or IBC versions of BTC or ETH
- a stablecoin

The choice of which of these assets to denominate payments is in practice a choice about whether each or both of the parties to the ICS agreement are willing to bear the exchange rate risk of the payment asset *vis a vis* ATOM and (particularly salient for validators) local fiat currency. Exchange rate fluctuations can impact the actual compensation received, potentially leading to financial disparities. Addressing this challenge is crucial for the financial health and stability of ICS.

The fundamental issue is whether the Cosmos Hub wishes to accept foreign exchange risk should the payment token diverge in price from ATOM. This is one of the most significant risks to the success of an ICS agreement: the value of the payment token dropping such that it is uneconomical for validators to continue to validate the consumer chain and thus putting their participation in validation of the Cosmos Hub under question.

Let us imagine the ideal approach from the Cosmos Hub's perspective. At the first instance, this could be a stablecoin (after all, validators are likely to pay for their equipment and other services in fiat currency). The payment would be structured such that it paid for the services produced: so rather than a revenue share model, the payments would be a fee-for-service one based on block production.

However, insisting on stablecoin payments could impose significant and unviable a cost on the consumer chain, potentially requiring them to exchange their transaction fee token to stablecoin and shifting the foreign exchange risk to the consumer chain. The consumer chain would be correct to insist on a discounted payment to the Hub to compensate for that risk. Likewise, a consumer chain would find a fee-for-service model would be difficult to commit to when the success of the chain is uncertain.

A more realistic and reasonable model is to require payment in ATOM. This has the advantage of reducing foreign exchange risk (ATOM price could go up or down but validators and ATOM holders are already exposed to this risk) and providing additional demand for the ATOM token. However, it is most suitable for chains that are already using ATOM as a fee token.

This discussion highlights a basic question underpinning how the onboarding of consumer chains that has not been adequately explored in the community: **what sort of business is ICS?**

We propose that there are two distinct ways to think about ICS relationships: as an infrastructure relationship, or as a venture relationship.

6.2. Infrastructure or venture?

If we think of ICS as **infrastructure relationships**, then consumer chains are buying specialised services of the Cosmos Hub to generate new, predictable and ongoing revenue streams. The Cosmos Hub is selling or leasing high quality and comparative low cost security to consumer chains and in return receives some stable income. Put another way, the Cosmos Hub is a service provider. There are all sorts of benefits from this relationship of course (such as alignment with the Hub and all the consumer chains within) but fundamentally to think about ICS as an infrastructure business is to think about it as service provision, and it should be priced as such.

Alternatively, the community might think of ICS as a **venture relationship**. In this way of thinking, the Hub is providing security as part of its investment in a sovereign chain, in the same way that venture capital provides advice and networking for firms it invests in. Through ICS the Cosmos Hub can support smaller chains and receive upside (or downside) on those relationships. Here, the objective for the Hub is not primarily about ongoing stable revenue, but rather that the Hub will make potentially loss-leading investments (e.g. subsidising the security of chains) while hoping for future potential upside.

The way that the Cosmos Hub views their relationship with any given consumer chain changes the way they should structure those agreements. The relationship type impacts the effective agreement structure both because (1) the objectives of the agreement differ; and (2) the fundamental risks of the agreement differ. That is, the structure should be guided by different contracting risks that come along with each chain, and the different purposes of the contract is to achieve different things. From this perspective we can start to think through what structures are available to different types of relationships (e.g. fee for service vs revenue share vs token swap).

Nevertheless, we propose that the design of all agreements should be guided around two aims. First, that the relationship is mutually beneficial: everyone should stay happy. Second, that the relationship should be structured to mitigate hazards: mitigate the unique contracting risks/hazards of the relationship that result in the relationship to collapse (either in vertical integration or exit).

While each agreement will address some common headings — payment terms, governance processes, exit clauses — the features of each of these will differ. We outline these broad headings as a template in the recommendations section of this paper.

If we think of ICS as infrastructure relationships, then (downside) foreign exchange needs to be mitigated. Ideally, payment for service would be in a token that maximises stability, and therefore the stability of revenue. This could be ATOM, a stablecoin or a generally accepted medium of exchange. Alternatively, if the payment is made in a native token, the payment quantity of that could be denominated separately (e.g., USD$1 worth of the native token), although this would require significant oracle reliance. By design, the infrastructure approach means that the Cosmos Hub fails to capture the upside of a consumer chain's success but at the same time it is (modestly or entirely) protected against the downside. The pricing models ought to be structured around recovering the marginal cost of validation as well as the opportunity cost of the resources deployed.

Viewing ICS as a venture relationship makes for very different considerations. For a venture relationship, the foreign exchange risk is a positive — the Cosmos Hub wants to be exposed to an asset that it believes has a likelihood of success. Thus, as noted above, the Hub would be seeking to acquire significant quantities of the consumer chain's native token as early as possible in the relationship (minimising the 'entry price' of the investment). The potential failure of that asset is a known hazard in investing and is mitigated by ensuring that there are a lot of 'bets' out in the market. For the venture approach, the Hub should be seeking to onboard a significant number of consumer chains (say 10-20). Venture relationships are speculative and are not expected to return revenue to investors until a moment of exit.

It's crucial to acknowledge that validators often bear a disproportionate cost when it comes to decisions related to foreign exchange risk and other aspects of shared security. Their role in ensuring the integrity and trustworthiness of transactions places them at the frontline of potential risks and challenges. Indeed, concerns have been raised about the impact of ICS on the microeconomics of validation, including the potential risk of centralisation.[48] Even if framed as a venture relationship the cost of onboarding borne by validators remains — thus some external party (either the consumer chain or the Cosmos Hub itself) might seek to compensated the validators for their work, or some part of the investment returns might be ring fenced to provide bonus rewards to the validators should the consumer chain succeed.

An additional factor if ICS is structured as a venture relationship is the need to realise the value of the investments. To the extent that the Cosmos Hub takes ownership of the native chain's assets above and beyond what is distributed to validators and delegators, the Cosmos Hub community will need to sell (or otherwise distribute) the assets so that the capital (and, hopefully, profit) can be deployed. Both consumer chain and Cosmos Hub will need to form the agreement with the expectation that any assets held by the Cosmos Hub will be sold.

7. Compensation models

7.1. Types of compensation models

There are many mechanisms which can be part of an ICS relationship, only some of which have been adopted in the ICS relationships thus far. Note that these are not mutually exclusive (e.g., a revenue share model could be matched with a one-time payment). We summarise a selection of these potential compensation mechanisms in the table below.

Compensation type	**Considerations**
Revenue Share	The consumer chain pays a share of their revenues to the producer chain. Revenues could include transaction fees, inflation, MEV revenue, and so on. Those revenues may change over time as the chain evolves (both in terms of the types of revenues a chain receives, and the volume of revenues). Revenue share could be paid in either ATOM or the native token of the consumer chain (if they

[48] See Chorus One Research (2023), 'Consumer Chain on-boarding and centralization - Chorus One Research', *Cosmos Hub*, June, https://forum.cosmos.network/t/consumer-chain-on-boarding-and-centralization-chorus-one-research/10927

	have one) or any other digital asset. This model aligns the interests of both parties: as the consumer chain's revenue grows, so does the compensation to the security provider, ensuring that security provisions scale with the chain's success.
Fee for service:	Consumer chains pay a price per transaction (or some other defined unit) in either ATOM or the native token of the consumer chain. Rather than sharing revenue, consumer chains might opt for a more transactional approach, such as: 1. payment per validation (every time a transaction is validated within the consumer chain, an ATOM-denominated fee is paid to the provider); 2. consumers chains make a payment per epoch for security services rendered during that epoch; 3. payment per fixed time period (similar to the epoch-based payment but more time-centric, consumer chains would pay for security services based on fixed time intervals, like monthly or annually).
Token swap (or 'interlocking treasury')	The consumer chain and producer chain undertake a treasury token swap, where they swap their own native assets in some determined ratio (e.g. ATOM for the native asset of the consumer chain). This involves intertwining the financial reserves of the consumer and producer chains. The different parties could use those swapped assets to generate yield. This arrangement not only provides a potential revenue stream but also more deeply financially integrates the chains. At a broader level this approach also indirectly links different consumer chains with interlocking treasuries (if they both hold ATOM).
Bond	The consumer chain passes control of a quantity of a yield generating asset (such as staked ATOM) to the Cosmos Hub. The generated yield is owned by the Hub. When the relationship between the consumer chain and the Hub ends, the bond is returned. If the consumer chain violates the terms of any of its agreement, the bond can be slashed or confiscated. This is obviously most suitable for agreements that have a fixed term, and there are a range of governance challenges over the bond throughout the agreement.
One-time payment	The consumer chain makes a large upfront payment for ongoing security provision. This is most useful where there are high fixed costs for onboarding.
Debt	The consumer chain borrows a valuable asset up front from the Cosmos Hub (e.g. ATOM), and pays the principal and interest down over time.

7.2. Deciding between compensation models

As these examples suggest, these mechanisms are highly dependent on the economic characteristics of the chain — as well as the availability of enforcement mechanisms. Every chain in the AEZ is sovereign, so ultimately a consumer chain can always end its relationships

with the Cosmos Hub. But that also gives the consumer chain flexibility to change its revenue sources in a way that might disfavour the Cosmos Hub. Mechanisms should be chosen with an eye to minimising the governance risks embedded in contractual relationships with fully sovereign counterparties.

While there are multiple avenues for consumer chains to compensate for shared security, each comes with its set of benefits, challenges, and considerations. It's essential for both parties to carefully evaluate these mechanisms, ensuring that they align with their operational needs, financial health, and long-term objectives.

Following on from the infrastructure versus venture discussion previously in Section 6.2, the nature of the consumer chain shifts how compensation should be structured.

The infrastructure approach: Those consumer chains that constitute an infrastructure relationship for the Hub will tend to be more established chains (rather than launching as consumer chains), have less expected variance in their project revenues, and may already have an established or clear user base and business model. This enables more effective pricing of the ICS agreement (although of course significant uncertainty remains).

In general the nature of an infrastructure relationship suggests that the compensation type should tend towards:

1. revenue share model (or fee for service model) rather than some more complex model of interlocking treasuries or airdrops
2. compensation ideally paid in either ATOM, a stablecoin, or another medium of exchange, or paid in a native token but denominated in the former
3. marginal cost pricing

An infrastructure relationship could differ in several ways to meet the objectives outlined earlier:

- The revenue share model can be set on a declining schedule, with higher revenue share in early periods and lowering as the consumer chain (potentially) grows.
- The revenue share can be stepped, with a higher rate until some fixed cost for the validators is paid off (e.g. there is rate prior to some value being paid off, and then rate declines once that is paid).

The venture approach: Those chains that constitute a venture relationship for the Hub will tend to be more appropriate for new or smaller chains with upside speculative potential. The purpose of these relationships for the Cosmos Hub is to take on risk with onboarding consumer chains. Note that this risk constitutes the opportunity cost of onboarding (i.e. the Hub could be onboarding a different chain) but also the fixed costs that are borne disproportionately by the validators.

If a proposed consumer chain primarily fits the category of a venture relationship, then the relationship should tend towards:

1. a token swap or interlocking mechanism to align incentives;
2. compensation in the native token of the consumer chain.

Compensation for ICS should be taken in an asset that will appreciate if the consumer chain is successful. The most direct approach to this is a token swap, where the Cosmos Hub exchanges

ATOM, which can be used by the consumer chain to support development, for the chain's native token as early as possible.

Some mechanisms are less appropriate or useful for venture-based relationships. For example, the Hub and consumer chains should be wary of imposing fees on chains that it wishes to maximise the upside on as any such fees may shrink the path to success for that chain. Venture investments are long term and do not typically involve the imposition of direct costs on the invested entity, not least from the moment of their creation.

8. Recommendations

In this section we provide a series of recommendations for the Cosmos Hub in developing and maintaining robust relationships in ICS. These recommendations emerge from the application of the economics of governance and contracting to the frontier problems of ICS.

8.1. Agreement-level governance body (sub-DAOs)

A robust and transparent governance mechanism between each consumer chain and the Cosmos Hub is paramount. Without a structured governance framework, the relationship risks suffering from misunderstandings, conflicts, and inefficiencies. Governance must consider the need for adaptation from both sides. There are many types of adaptation. Some changes are simple or operational, such as the need to reprice the agreement (e.g. the precise % of revenue share). There may be broader unforeseen challenges (e.g. the costs of validation shift, consumer chain launched a new product or native token). There is also the ongoing threat of opportunism, where either party may act in their own interests to gain advantage, threatening the breakdown of the ICS relationship.

ICS relationships should be designed to be robust to changes in conditions. ICS governance relationships should aim to be mutually beneficial through robustness. That is, these relationships remain economically sustainable for both parties and do not fail to adapt (e.g. leading to integration with the producer chain, or unwanted exit). Careful governance design can mitigate some of the frictions we outline above. As ICS evolves, we anticipate further mechanisms (e.g. treasury swaps, hostages) to be developed that mitigate some governance costs.

We recommend that each ICS agreement should implement a governance body at the level of that agreement. That body should represent the interests of both the consumer and producer chains over time, including undertaking regular review processes.

There are two broad structures that a governance body for ICS could take:

1. **An overarching governance body.** The first approach is one governance body representing all of the ICS relationships at a given point in time. This model is more holistic, where a single body oversees the multiple (and expanding) ICS relationships of the AEZ. This approach is particularly beneficial if there's significant synergy or overlap among the relationships or if there's a need for a unified governance approach.

2. **A relationship-specific governance body.** The second approach (our recommended approach) is to develop a governance body at the specific level of an ICS agreement. An alternative term for this is a subDAO that represents each ICS relationship. That is, each individual producer-consumer chain ICS relationship has a governance body. This

approach, as we outline below, is preferred because it facilitates local knowledge and polycentricity, enables discussions (at least initially) in private, and because there are limited externalities across consumer chains.

Why do we recommend that governance bodies sit at the level of an ICS agreement? First, local knowledge. A lower-level governance body draws on the local contextual knowledge of the chains in that agreement. There are of course many details about ICS agreements that are not broadly understood by the Cosmos community. Long term contractual agreements have both explicit and implicit elements that cannot easily be understood by outsiders. A polycentric system of governance, with many smaller governance bodies, is more conducive to revealing this local knowledge.

Second, enables private negotiation and good faith discussion. Often negotiations best occur in a private and lower-stakes environment. This enables parties to the contract to air their concerns, for instance without creating a public forum post that is accessible globally. Of course, neither of these points suggest that decisions should not be ratified by all ATOM token holders (and indeed the governance of the consumer chain), but that at least some governance will occur in a more private lower stakes environment.

Third, limited externalities across consumer chains. The decision of an overarching or relationship-specific governance body can also hinge on the externalities (or spillover effects) introduced by the shared security arrangements. If there were significant externalities between consumer chains, then a unified governance model may be appropriate. In this instance an overarching governance body for all ICS relationships would address these externalities from a whole of AEZ approach. But if the externalities are limited to specific or individual relationships, then there is greater value in a lower-level agreement. Shared security arrangements would generate limited, if any, externalities across the governance bodies.

8.1.1. Governance body structure

Taking the need for a relationship-specific governance ICS governance body as given, how should those bodies be structured? Partly this will depend on the nature of the specific agreement. The precise structure of each of the governance bodies can be customised to reflect the needs and demands of each ICS agreement. However, in the table below we propose a committee that has representatives from the consumer chain, producer chain and the validator set. Each of these members might be proposed in the initial proposal to join the AEZ.

Governance Body Representatives	**Number**	**Details**
Cosmos Hub token holder representatives (producer chain)	2	Chosen through Cosmos Hub governance. Role: To represent the interests of the Cosmos Hub token holders.
Consumer chain representatives	2	Chosen by consumer chain governance process, and potentially proposed in onboarding process. Role: To represent the interests of the consumer chain's community

Cosmos Hub validator representatives	2	Chosen through Cosmos Hub governance. Role: To represent the interests of the Cosmos Hub validators. Ideally 1 representative from the top and bottom half of the validator set.

It's worthwhile noting the likely need for information sharing about consistency and best practices across each ICS-level governance bodies. There are several ways this could be facilitated. For instance, there would be common representatives from the Cosmos Hub or the validator set that have visibility over multiple ICS relationship. Alternative, governance bodies could include individual independent members solely for the purposes of information sharing. Furthermore, we have not here dealt with the question of how these representatives are compensated, which is a matter for each of the individual chains and communities to determine.

The extent to which these governance decisions are executed is partly a technical problem, and how that occurs will evolve over time. In the short term we anticipate these bodies to be off-chain governance committees. Their role is to meet and make decisions relating to their specific ICS agreement. For instance, in a regular review, the governance body may determine the need to reprice the percentage of revenue share, or to alter the asset compensation is paid in. Where necessary, the outcomes from those governance body agreements would be proposed to the Cosmos Hub and voted on-chain by token holders. These governance bodies could make recommendations to the Cosmos Hub through proposals, where token holders would vote on the suggested changes (if any).

Future infrastructure developments in Cosmos will enable more bespoke governance arrangements. This will transition these bodies to align more closely with the terminology of subDAOs. The cryptodemocratic design space within which we can innovate on governance structures is expanding as we develop more DAO architecture on the Cosmos Hub and more broadly.[49] We anticipate greater capacity for delegation of powers, including the unbundling of different governance rights. Some of these arrangements may better, and perhaps more efficiently, maintain the sovereignty of token holders on both chains. For instance, we may enable more direct election of governance body representatives from the producer or consumer chains. Other models might draw token holder perspectives into ICS governance decisions at particular points in time.

The question of what decisions are made by the ICS governance body and what requires the voting of token holders is one of constitutional design.[50] For instance, the governance bodies could be delegated the right to make decisions about specific governance powers, such as changing the pricing agreement within some set bound. Other more major decisions, such as changing the compensation asset from ATOM to the consumer chains, may sit outside the remit of the governance body and always require some form of token holder vote. We also expect that where powers are delegated to the governance body, mechanisms of token holder veto or

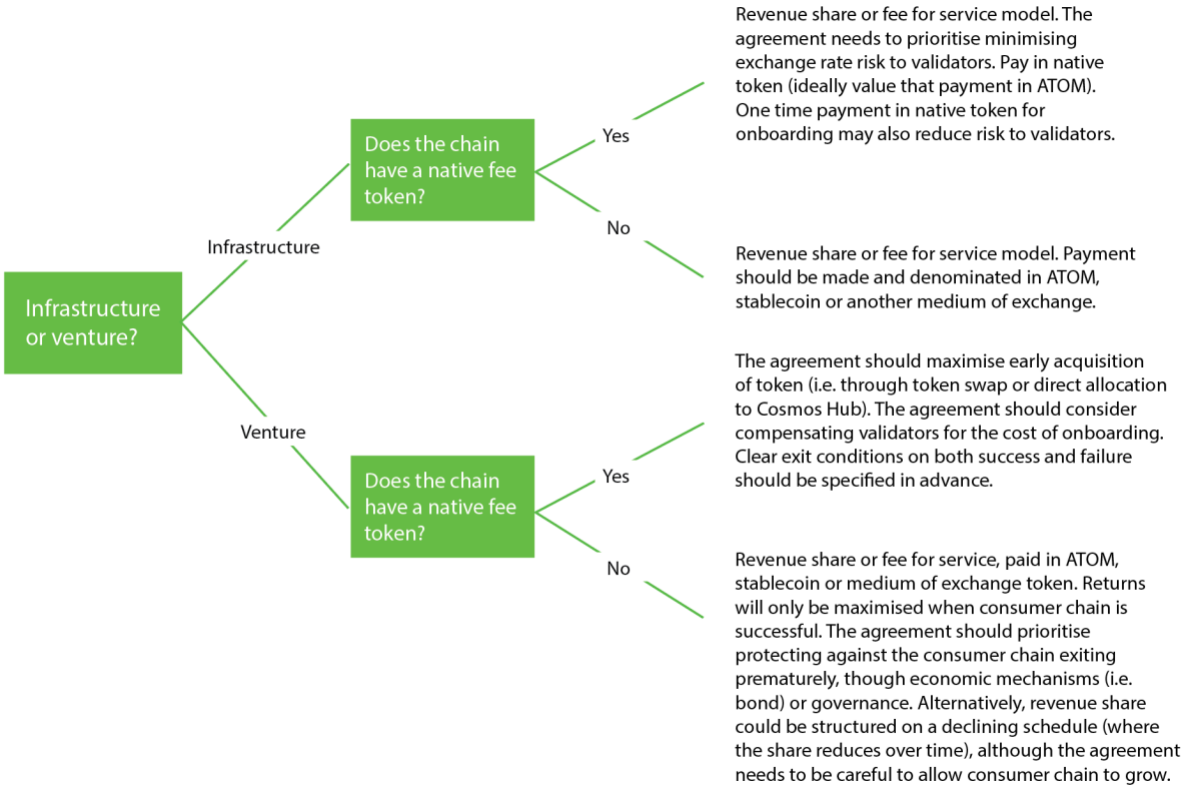
[49] Darcy W.E. Allen, Chris Berg and Aaron M. Lane (2019). *Cryptodemocracy: How blockchain can radically expand democratic choice*. Rowman & Littlefield.

[50] On constitutions and blockchains see, for instance, Alston, E. (2020). Constitutions and blockchains: Competitive governance of fundamental rule sets. *Case W. Res. JL Tech. & Internet*, 11, 131. Alston, E., Law, W., Murtazashvili, I., & Weiss, M. (2022). Blockchain networks as constitutional and competitive polycentric orders. *Journal of Institutional Economics*, 18(5), 707-723.

disallowance will be developed. For instance, while the governance body has the right to make some minor decisions, a broader set of token holders might have the right to disallow or veto the decision within a period of time.

8.2. A decision tree

Here we provide a high-level decision tree to guide approaches to ICS agreements. The two paths are whether the agreement is to have an infrastructural or venture basis and whether the consumer chain has a native fee token that can be used for the purposes of the ICS agreement.



8.3. Onboarding template: governance and length of agreement

In this section we propose an onboarding template for consumer chains. This is intended as a template and a guide to consumer chains, rather than a firm requirement. We understand that each individual proposal will be different, but there is value in lowering the transaction costs of onboarding. Our focus is on integrating mechanisms that facilitate onboarding as well as mitigating some contracting hazards through governance. Before we outline the template, it is useful to briefly explore the merits and importance of (1) regular review touchpoints; and (2) the need for specific exit and conflict resolution mechanisms.

8.3.1. The need for regular review touchpoints

Governance changes can significantly impact the shared security framework, especially if they affect either payments (e.g. changes in the asset, or reasonable nature of terms) or the producer chain's operational aspects. Major shifts in either the producer or consumer chain, especially ones that might adversely impact the producer chains capacity to produce security long-term,

must be adequately addressed through governance. This could include actions that erode trust, introduce vulnerabilities, or undermine the operational efficiency of the agreement overall.

ICS agreements need designated periods for renegotiation. Both the consumer and the producer chain need points where they can revisit and recalibrate their terms, ensuring that the relationship remains equitable, relevant, and mutually beneficial. In the first instance, open-ended set-and-forget agreements exacerbate many of the contracting hazards outlined throughout this paper, potentially leading to agreement collapse or vertical integration.

One solution to open ended agreements, and perhaps the more extreme version, is to directly constrain the length of ICS agreements by making them fixed term. There will likely be some trepidation about this, and limiting agreements in this way also creates challenges (e.g. it can itself manifest hold-up problem issues). There are also the obvious fixed costs of integration by both the consumer chain (e.g. where they have made the choice to use the Cosmos SDK) and the producer chain (where the validators have paid fixed costs of integration, such as through the deployment of new hardware). Nevertheless, one option is to directly limit the length of ICS agreements and require consumer chains, if they wish, to propose to join the AEZ again (or exit) at the conclusion of that agreement.

A more appropriate approach sits in between open-ended agreements and fixed term agreements: **regular review touchpoints**. Regular review touchpoints provide an opportunity for consumer and producer chains to reassess, renegotiate, or even dissolve the relationship if it is not serving mutual interests. Review touchpoints include the potential for both routine updates and renegotiation. For the former, continuous communication between the parties is essential. This communication builds trust and allows for proactive management of issues. For the latter, the dynamic nature of the relationship between the producer and consumer chain might need significant renegotiation. These renegotiations enable the relationship to remain relevant and mutually beneficial, including ameliorating the hazards of vertical integration and opportunism discussed earlier.

The need for regular review processes will be ICS relationship specific. A default might be one year for a review of the agreement. The cadence of review touchpoints should directly relate to the nature of the underlying consumer chain (e.g. the stage and potential scale of the consumer chain shifts the likely need for adaptation). ICS proposals should also consider processes for triggering renegotiation in the face of unexpected changes outside of the review window, as well as the potential clauses for exiting the agreement. We recommend operationalizing these processes through the agreement-level governance body, such as through the option for a certain percentage of votes in the governing body to lead to a renegotiation process, or other triggers such as a token holder vote of either chain (i.e. if either the Cosmos Hub token holders or the native chain token holders, if applicable, can trigger renegotiation).

8.3.2. Exit and conflict resolution conditions

For the longevity and stability of shared security relationships, explicit exit conditions must be established. Exit conditions offer clarity on how and under what circumstances a consumer chain can disengage from the shared security arrangement, ensuring orderly transitions and minimal disruptions. While governance through the ICS level governance agreement (combined with clear contractual terms through the proposal) will reduce some governance frictions, disputes will inevitably arise. Each ICS agreement should have predefined conflict resolution mechanisms. There are various ways that these dispute resolution mechanisms could be

structured. For instance, third-party arbitrators familiar with blockchain, or even the emergence of decentralised dispute resolution mechanisms.

8.3.3. An onboarding template

Not every agreement will use the below template. It provides a recommended starting point to make the governance processes of onboarding clearer for both parties, including drawing attention to the critical issues of compensation and governance. It also directs attention more specifically to the contractual arrangement between the two parties rather than the business model of the consumer chain.

Title	**Description**
Title	Proposal title
Summary	A concise summary of the proposed ICS relationship, including the compensation terms for shared security services.
Parties to the agreement	Defines the parties to the ICS agreement.
Description of the consumer chain	Introduces the consumer chain that is proposing to join ICS. This should avoid an excessively detailed outline of the consumer chain. The audience should be assumed to be non-technical. In introducing the consumer chain consider the following questions: ● Is the consumer chain an existing chain or is it launching on ICS? ● What are the core business and revenue models of the consumer chain? ● Does the consumer chain have a native token (or a roadmap to introduce one)? If so, what are some of the basic token economics details (e.g. supply, allocation)? ● What is the current governance structure of the consumer chain? ● Has the consumer chain undertaken security audits or other testing (e.g. participation in testnet)? ● Does the consumer chain have any relevant partnerships or collaborations within Cosmos?
Scope of services provided	Identifies the security services being provided by the Cosmos hub (e.g. validator services, maintenance). *Scope and details of services* ● Are there estimates of the volume of security services needed (e.g.

	transaction volumes)? ● Are there requests from the Cosmos Hub aside from security provision (e.g. ATOM into a liquidity pool)? ● Are there relevant governance considerations for the compensation arrangement (e.g. governance of a liquidity pool)? *Services performance* ● What are the relevant performance standards from both sides of the agreement? ● Are there relevant quantifiable metrics of performance?
Compensation model	A clear breakdown of the compensation arrangement provided by the consumer chain to the producer chain (e.g., X% of transaction fees, inflation, MEV revenue). Clearly indicate how compensation will be calculated (e.g. timing) and how payment will occur. Provide details on how the compensation model has been developed (e.g. costings and predictions of compensation) including the choice over alternative models. Distinguish clearly between current sources of compensation (i.e. what will occur immediately on entry to AEZ) and future potential sources (e.g. revenue from future products). If relevant, provide any specific terms that would trigger some renegotiation of the compensation model (e.g. new revenue streams on the consumer chain, size of pricing moves, deviation from expected levels of compensation).
Asset(s) of Payment	What asset is the compensation described above paid in (e.g. ATOM, native token, stablecoin)? Explain why this has been chosen as the approach. For assets other than ATOM provide some details about that token (e.g. supply, inflation, governance, history). Consider including a risk analysis of the token.
Duration of agreement	Explicitly defines the duration of the agreement (e.g. open ended, fixed term, automatic renewal).
Implementation and details	Any specific implementation details of the agreement. Include timelines and processes for if the agreement were to be approved.
Dispute resolution	Describe the processes by which disputes will be resolved. The first process by which disputes are resolved should be through the ICS level governance body.

Establishment of a governance body	Details the establishment of a governance body for the ICS agreement (see section 7.1 above). This could include answering questions such as: ● What is the objective of the governance body? ● How many members? ● What is the structure of membership across different ecosystems (e.g. representatives from the Cosmos Hub and consumer chains)? The proposal may name specific representatives that will sit on the governance body. ● What are the proposed governance processes (e.g. yearly reviews of the contract agreement)? ● What is the proposed compensation (if any) for members of the governance body? ● Are there any independent members on the governance body?
Termination	Detail exit conditions for the agreement, including the consequences of such termination for either party. These consequences may be different given the time that the termination occurs following the beginning of the agreement.
Miscellaneous	Any other important details or clauses relevant to the agreement.
Links and other references	Links to relevant documentation

9. Conclusion

In this paper we have applied existing institutional economics theory to the frontier governance problems of interchain security (ICS) in Cosmos. Our aim has been to create more robust and sustainable governance structures of ICS relationships and to ensure that these economic relationships are mutually beneficial. We have made several recommendations including:

- The implementation of agreement-specific ICS agreements that enable these agreements to adapt and evolve to changing conditions.
- The use of a decision tree for the Cosmos Hub through the lens of infrastructure or venture relationships.
- Consumer chains should use an onboarding template to lower the costs of onboarding, including the need for regular review touchpoints and exit and conflict resolution mechanisms.

We have not provided specific prescriptive rules in this paper. Rather, we have focused on the core principles by which individual ICS relationships can be developed, and the costs of buying

security rather than making it can be reduced. There are several reasons for this principles-based approach.

- First, ICS will evolve over time in unpredictable ways. As further evolutions of ICS introduce new complexities (e.g. mesh, opt-in and layered shared security models) the way that we govern these relationships will also need to evolve. We will also have a greater technical design space for evolving ICS relationships.
- Second, each ICS relationship is context specific. While the theoretical frameworks of governance can provide overarching guidance, the pragmatic reality is that each ICS agreement is unique, emerging from a complex relationship between consumer and producer chain communities.
- Third, much of the knowledge about how to best govern ICS agreements will be understood through trial and error experimentation. We are trying to govern relationships in a digital context, across organisational boundaries, and with frontier technologies. Over time the empirical evidence gathered from applying ICS in practice should inform the design of robust governance models that can adapt to the changing landscape of ICS agreements.

Our findings and recommendations in this paper are the foundations of an ongoing research program into interchain security and shared security more broadly. We have raised many questions about the structure of ICS agreements, and we anticipate a broader theoretical and empirical toolkit to be applied over coming years to answer more specific questions (e.g. optimal parameters of agreements).

References

0xspaydh (2023) 'Replicated Security and Why it Matters for Cosmos', HackerNoon, 25 April, https://hackernoon.com/replicated-security-and-why-it-matters-for-cosmos

Alston, E. (2020). Constitutions and blockchains: Competitive governance of fundamental rule sets. Case W. Res. JL Tech. & Internet, 11, 131.

Alston, E., Law, W., Murtazashvili, I., & Weiss, M. (2022). Blockchain networks as constitutional and competitive polycentric orders. Journal of Institutional Economics, 18(5), 707-723.

Allen, Darcy. W. E, & Potts, Jason. (2023). 'Web3 toolkits: A user innovation theory of crypto development'. Journal of Open Innovation: Technology, Market, and Complexity, 9(2), 100050.

Allen, Darcy W.E, Chris Berg and Aaron M. Lane (2019). Cryptodemocracy: How blockchain can radically expand democratic choice. Rowman & Littlefield.

Aoki, M. (1983). Managerialism revisited in the light of bargaining-game theory. International Journal of Industrial Organization, 1(1), 1-21.

Barzel, Y. (2002). A theory of the state: economic rights, legal rights, and the scope of the state. Cambridge University Press.

Berger, P. G., & Ofek, E. (1995). Diversification's effect on firm value. Journal of Financial Economics, 37(1), 39-65.

Besanko, D., Dranove, D., Shanley, M., & Schaefer, S. (2009). Economics of strategy. John Wiley & Sons.

Buchman, Ethan and Hart, Sam "The Cosmos Hub is a Port City" https://blog.cosmos.network/the-cosmos-hub-is-a-port-city-5b7f2d28debf

Chorus One Research (2023), 'Consumer Chain on-boarding and centralization - Chorus One Research', Cosmos Hub, June, https://forum.cosmos.network/t/consumer-chain-on-boarding-and-centralization-chorus-one-research/10927

Coase, R. (1937) 'The Nature of the Firm', Economica 4(16): 386-405

Coase, R. H. (2000). The acquisition of Fisher Body by general motors. The Journal of Law and Economics, 43(1), 15-32.

Cosmos Christina (2023) 'Interchain Security Begins a New Era for Cosmos' 17 May, Cosmos Network Blog https://blog.cosmos.network/interchain-security-begins-a-new-era-for-cosmos-a2dc3c0be63

Cosmos Hub (2023) 'Comparing Replicated, Opt-in, and Mesh Security' The Interchain Foundation Medium, 23 May, https://medium.com/the-interchain-foundation/comparing-replicated-opt-in-and-mesh-security-a24d67e04b81

FitzRoy, F. R., Acs, Z. J., & Gerlowski, D. A. (1998). Management and economics of organization. Prentice Hall.

Gigerenzer, G. (1997). Bounded rationality: Models of fast and frugal inference. Swiss Journal of Economics and Statistics, 133(2/2), 201-218.

Hillier, B. (1997). The economics of asymmetric information. Bloomsbury Publishing.

Klein, B. (1998). The hold-up problem. The New Palgrave Dictionary of Economics and the Law, Peter Newman, ed., Macmillan Reference Limited.

Klein, P. G. (2005). The make-or-buy decisions: Lessons from empirical studies. Handbook of New Institutional Economics, 435-464.

Klein, B., Crawford, R. G., & Alchian, A. A. (1978). Vertical integration, appropriable rents, and the competitive contracting process. The Journal of Law and Economics, 21(2), 297-326.

Langlois, R. N. (2023). The Corporation and the Twentieth Century: The History of American Business Enterprise. Princeton University Press.

Milgrom, P. & Roberts, J. (1992). Economics, organization and management. Englewood Cliffs, NJ: Prentice-Hall.

Peltzman, S. (1976). Toward a more general theory of regulation. The Journal of Law and Economics, 19(2), 211-240.

Rennekamp, Billy (2021) 'Interchain Security is Coming to the Cosmos Hub', Interchain Ecosystem Blog, 1 September https://blog.cosmos.network/interchain-security-is-coming-to-the-cosmos-hub-f144c45fb035

Riordan, M. H., & Williamson, O. E. (1985). Asset specificity and economic organization. International Journal of Industrial Organization, 3(4), 365-378.

Scott, R. E., & Triantis, G. G. (2005). Incomplete contracts and the theory of contract design. Case Western Reserve Law Review 56, 187.

Simon, H. A. (1997). Models of bounded rationality: Empirically grounded economic reason. MIT press

Shleifer, A., & Vishny, R. W. (1991). Takeovers in the'60s and the'80s: Evidence and implications. Strategic Management Journal, 12(S2), 51-59.

Tremback, Jehan (2022) 'An Overview of Interchain Security v1', Informal Systems Blog, 2 February, https://informal.systems/blog/interchain-security-v1

Tremback, Jehan, Marius Poke, Juan Beccuti (2022), ' Replicated vs. Mesh Security' Informal Systems Blog https://informal.systems/blog/replicated-vs-mesh-security

Tremback, Jehan (2022) 'Building With Interchain Security' Informal Systems blog, 9 May, https://informal.systems/blog/building-with-interchain-security

Williamson, O. E. (1979). Transaction-cost economics: the governance of contractual relations. The Journal of Law and Economics, 22(2), 233-261.

Williamson, Oliver (1985) The Economic Institutions of Capitalism. Free Press: New York.

Williamson, O. E. (1993). Opportunism and its critics. Managerial and Decision Economics

WillB (2023) “Enabling the ATOM Port City”, Cosmos Hub Forum, 27 October https://forum.cosmos.network/t/enabling-the-atom-port-city/11909