NAORIS PROTOCOL

WhitePaper

CyberSecurity Mesh HyperStructure for the Digital World

Authors: David Carvalho, Sumit Chauhan
Date: 02/02/2022
Version: 1.02.02

1.0. Abstract

We are Naoris Protocol, the CyberSecurity Mesh HyperStructure[1] for the hyper connected world, leveraging the best of Ethereum and conceived to run in a multichain world, forever.
Naoris Protocol's disruptive and contrarian design pattern makes networks safer as they grow, not weaker, by turning each device into a trusted validator node.

Having been finalists in over half-a-dozen top rated business and innovation accelerators around the world, Naoris Protocol was conceptualized and founded to tackle the most critical areas of business and governance by a team with decades of experience and thought leadership in CyberSecurity. Naoris Protocol promises to revolutionize how security is approached, considered and implemented, allowing for safer information sharing environments, decentralization, and ultimately, industry-wide standardization.

As devices validate each other on a tokenized machine economy, single points of failure are eliminated and a trusted communication layer is established among devices in real time.
We exist to pioneer the vision of building a Decentralized CyberSecurity Mesh that is:

- Unstoppable
- Permissionless
- Minimally Extractive
- Valuable
- Expansive
- Positive Sum
- Credibly neutral

This, without relying on a myriad of legacy centralized, siloed solutions, which typically increase complexity and reaction time, while also expanding the attack surface area of networked systems.

Naoris showcases a novel consensus mechanism called Distributed Proof of Security (dPoSec), running on a purpose-built blockchain that can record 50k-1M processes, network state changes and general transactions per second. The protocol operates using a new sharding-like architecture that we call Verge Clusters. Verge Clusters carry case-specific security and compliance logic ensuring the integrity of all networks, devices and processes using the protocol.

Naoris Protocol is generalized yet powerful and customizable, providing value to nation states, governance structures, industries, Web2, and the entire Web3 stack. It's built for everyone without competing with existing L1 and L2 solutions. In fact, blockchain projects can adopt Naoris to avoid inheriting Web2 CyberSecurity risks, and to enhance the integrity of their own validators and nodes.

The protocol is community-governed, censorship resistant and conceived to change the game in CyberSecurity, while simultaneously mitigating a $10T per year problem by at least an order of magnitude.

In essence, Naoris is developing state-of-the-art, scalable blockchain technology that is built to address a critical concern of the digital world, and become adopted by all sectors of the economy. A pragmatic solution that can be deployed in the next few years, not decades - and one that can self-heal, expand and thrive for generations to come. With a sense of urgency, but also a strategic focus on the infinite game, our vision is to become the world's CyberSecurity mesh HyperStructure that enables the permanent neutralization of the cyber threat.

[1] https://jacob.energy/hyperstructures.html

2.0. Introduction

2.1. A New Era in CyberSecurity

CyberSecurity has finally met the blockchain, and the implications for the world of data security are momentous.

Naoris Protocol provides the world's first blockchain-based cyber-enforced mesh HyperStructure, bringing a game-changing platform to address 35 years' worth of industry practice through the unrivalled security potential of ethical blockchain use. Following the HyperStructure ethos of our use case, Naoris suggests a decentralized security enforcement protocol that is unstoppable, permissionless, minimally extractive and credibly neutral, with a win-win default baseline mentality. Every device becomes a cyber-trusted validator node, making networks safer as they grow, not weaker.

Global spending on CyberSecurity products and services has never been as high as it is today, being expected to exceed $1.75 trillion cumulatively for the five-year period from 2021 to 2025.[2] Despite this, cybercrime damages will cost users, companies, and governmental entities $10.5 trillion yearly by 2025, up from $3 trillion USD in 2015.[3]

Leveraging the benefits of blockchain technology, Naoris Protocol enables individuals and businesses to assert unprecedented control over their data and digital security. Bypassing traditional industry practice which makes use of potential single points of security failure like vendors, intermediaries and third parties, Naoris Protocol elevates the peer-to-peer format into a truly collaborative security infrastructure where an increased number of users results in enhanced, instead of reduced, digital security.

Naoris is a CyberSecurity ecosystem that is agnostic to device or operating system, meaning that it works on any networked device, whether smartphone, computer, or self-driving car. By harnessing the power of the infinitely scalable blockchain across a truly vast number of users, Naoris enables a reality where individuals and businesses can feel more secure as they carry out their everyday business, distributing cyber-resilience mechanisms through dPoSec, a CyberSecurity, assurance and trust dedicated consensus power structure.

The ultimate goal is for the default security solution to stop deferring to the creation of device and network silos - which themselves introduce significant risk factors - and instead gravitate toward a distributed, democratic trust-generating framework.

For much of the past half century, device and network security has operated on siloed principles, with most environments (regardless of criticality to society and business) based on centralization of data and processing. As such, each of the supporting devices within such ecosystems become a potential point of weakness, resulting in imminent failure in the event of any internal or external threat materializing.

This creates a high-risk state of existence, as the compromise of a single networked device would undoubtedly allow the attacker to gain access and control over an entire network of devices, their services and operational processes - allowing for abuse and/or subversion of all operational assets within the exploited level of access, whether the environment is a traditional business, industry, or a critical asset, such as a nation state agency or critical infrastructure.

Thus the threat actor has the capability to wreak havoc in terms of IP exfiltration and ownership of critical applications, and impersonation,

[2] https://CyberSecurityventures.com/CyberSecurity-spending-2021-2025/
[3] https://CyberSecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

becoming in effect an APT (advanced persistent threat). Such a threat could go undetected for weeks, months, years or indeed indefinitely - and be fully undetectable during that time.

Threat actors exploit business critical systems for personal profit, to further the agendas of certain groups or power structures, or as an act of cyberwar, cyber-terrorism or cyber-espionage. Regrettably, results generated by traditional siloed CyberSecurity frameworks frequently under-deliver. These same techniques and underlying weaknesses are the accepted standard, employed as current industry norms across Web2 and Web3 - making countless networks vulnerable to exploitation. **Current CyberSecurity solutions have yet to effectively address these threats.**

Naoris Protocol introduces fundamental changes to this traditional approach, addressing these persistent risks. Through bleeding edge CyberSecurity and blockchain technology, **Naoris Protocol turns centralized computer networks with traditionally untrusted devices into a decentralized cyber-secure mesh, where a swarm of cyber-trusted devices validate each other.**

Devices operate within a tokenized machine economy, where single points of failure are eliminated, and threats are identified and mitigated in near real time under a dedicated consensus model that rewards devices for consistent trusted behavior. Naoris Protocol is a genuine game-changer.

The company's objective is not only to exponentially improve data security and verification, but to play a fundamental role in the ongoing evolution of the CyberSecurity landscape and its future. Therefore, today's distributed threats demand a new kind of solution:

2.1.1. We're Building a HyperStructure.

The risk of systemic CyberSecurity failure cannot be solved by a traditionally framed company as the company itself could become a single point of failure for the integrity of the CyberSecurity mesh. Therefore, Naoris Protocol is a DAO governed protocol, using quadratic voting.

This vision for a HyperStructure that is a mission-critical piece of digital planetary infrastructure, built to run forever, requires 7 bold design principles:

1. **Unstoppable:** It runs indefinitely; devices and networks can adopt it or abandon it, but it cannot be stopped.

2. **Permissionless:** Users and builders cannot be deplatformed - it's censorship resistant and accessible by anyone.

3. **Minimally Extractive:** Near base cost fees disincentivize forking, while powering a treasury for ecosystem development managed by the DAO.

4. **Valuable:** Conceived to be a for-public endeavor, and yet, extremely valuable to own and govern - which sparks an ecosystem around it.

5. **Expansive:** It has built-in incentives for users to behave fairly, and for builders to build on top of it.

6. **Positive Sum:** Wide adoption and usage of the protocol results in a win-win environment for all network participants.

7. **Credibly Neutral:** To be adopted by a wide range of DAO-based governance structures, companies and individuals, HyperStructures need to be credibly neutral.

2.2 Historical Background of Distributed Systems

The notion of provable distributed truth, i.e. provable distributed integrity, has existed since the beginning of networked computing. The use of concurrent processes that communicate through message-passing had its origins in operating system architectures studied as early as the 1960s.

The Advanced Research Projects Agency Network (ARPANET) was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet.

The first widespread distributed systems were local-area networks, like Ethernet, which were devised in the 1970s. ARPANET itself, the predecessor of the internet, was released for testing in the late 1960s, and its email was devised in the early 1970s as a federated environment.

E-mail became the most prosperous program of ARPANET, and arguably the earliest example of a large-scale distributed application. The analysis of distributed computing, from a perspective of local architectures and networks, became its own branch of computer science.

2.3. Current Approach to Cyber Risk and Defensive Capability Stagnation

Within any corporate or critical environment, having a central point of governance should produce the assumption that any infrastructure will at some point be compromised, or vulnerable to falling prey to external power structures with their own agendas - if it is not in that state already. The fact is that trust is an asset that cannot be outsourced without incurring massive risk.

Despite this, circumstances are such that there is currently little alternative to accepting the risks that centralization and the intricacies offered by it, and/or accepting the risks that a third-party black box tool or collection of tools offers - along with the potential internal threats all the people operating those tools on the organization or client's behalf bring.

It should also be assumed that the current infrastructure is already compromised, or will be in the future, even if current best practice is achieved and duly validated. As such, the more crucial and valuable the resources at play - such as strategic plans, mergers and acquisitions and other important documents, intellectual property (IP), Personal Identifiable Information (PII) databases, payment card industry info P(CII), and so on.

The more sensitive the data, the more attractive it is to bad actors, and the higher the risk endangering this digital asset, the loss of which (if left unchecked) could lead to a survivability event for the business or at the very least high-impact monetary and/or reputational damage.

2017 was the year when a series of incidents in the cyber threat arena resulted in the definitive recognition of some universal truths. There was unwavering evidence regarding monetization procedures, attacks on democracies, cyberwar, transformation and abuse of malicious infrastructures, along with the dynamics contained in threat agent groups.

However, 2018 and the years after have also attracted successful operations against cyber-criminals, albeit insufficient. Law enforcement, governments and businesses have successfully shut down illegal dark markets, de-anonymized most of the Dark net and arrested many cyber-criminals. Moreover, state-sponsored campaigns were revealed and specific intelligence regarding such technologies deployed by nation states were also leaked, potentially benefiting the privacy of citizens and the rule of law, while allowing cyber criminals to have access to top nation-state level hacking tools.

This all contributes to making society more unsafe, and opening the way to cyber-terrorism and other disruptive and destructive cyber-threat actor capabilities - by 2022, risking incurring large damages transversally on democratic-social capabilities, critical infrastructure damage and subversion, ransomware of critical areas of society like healthcare and energy systems.
As a consequence trust levels in institutions were observed declining heavily, in parallel with obvious perceived and real-world risks. Inevitably public perceptions of the limited capability to prevent or even respond to such risks increased, despite the widening use of best-in-breed cyber tools and their wider dissemination and enforced cyber standards. Despite the lack of mitigation, data security has never had a higher public profile and awareness, a trend that will inevitably increase in the coming years.

The CyberSecurity community is struggling to maintain parity, in the endless arms race between defenders and attackers. Although every year the CyberSecurity industry has achieved records in security-related investments, they have also brought new documented cyber-attacks of automated and manual natures, global data breaches, and costly information loss and theft.

From this standpoint, there arguably is a market failure in CyberSecurity; that is, the fact that theoretically higher defense levels and higher associated expenses cannot successfully reduce levels of real world cyber threat exposure. Whether that is a result of a segmented CyberSecurity marketplace, lack of awareness, or capability, are themes of vibrant discussions in the corresponding communities.

The simple fact is, however, that in recent years, there has been a clearly documented increased quantity of information on the occurrence of malicious CyberSecurity events and cyberspace abuse, following year-on-year trends. This tendency is reflective of the high amount of interest by news online news services, web services and indeed across the whole Internet and traditional media regarding CyberSecurity problems.
In its 2022 Tech Trends, Gartner identifies CyberSecurity mesh as one of the core technologies the majority of the world's organizations will be using in the next few years, to address these vulnerabilities.

In summary, some of the main trends in the cyber threat landscape over the course of the last half decade were:

- Number of attacks and expertise of malicious actors in cyberspace continuing to increase;
- Malicious infrastructures keep evolving their capabilities involving multipurpose configurable functions for traditional cyber-defense subversion such as anonymization, detection and encryption evasion;
- Usage of decentralized ledgers as backbones for important threats such as botnets;
- APT Advanced Persistent Threats and FUD Fully UnDetectable threats are becoming the norm, increasing detection times on average for breaches to 280 days in average[4];
- State-sponsored attacks are one of the most omnipresent malicious threat agents in cyberspace and the top concern of governmental and commercial defenders. Traditional cyber-defense environments do not seem to be able to protect such high-value targets from advanced attacks;
- Cyber-war is entering heavily into cyberspace, creating increased worries to critical infrastructure and industry, especially in areas that are critical but legacy, or are in budgetary crisis or geopolitical crisis.

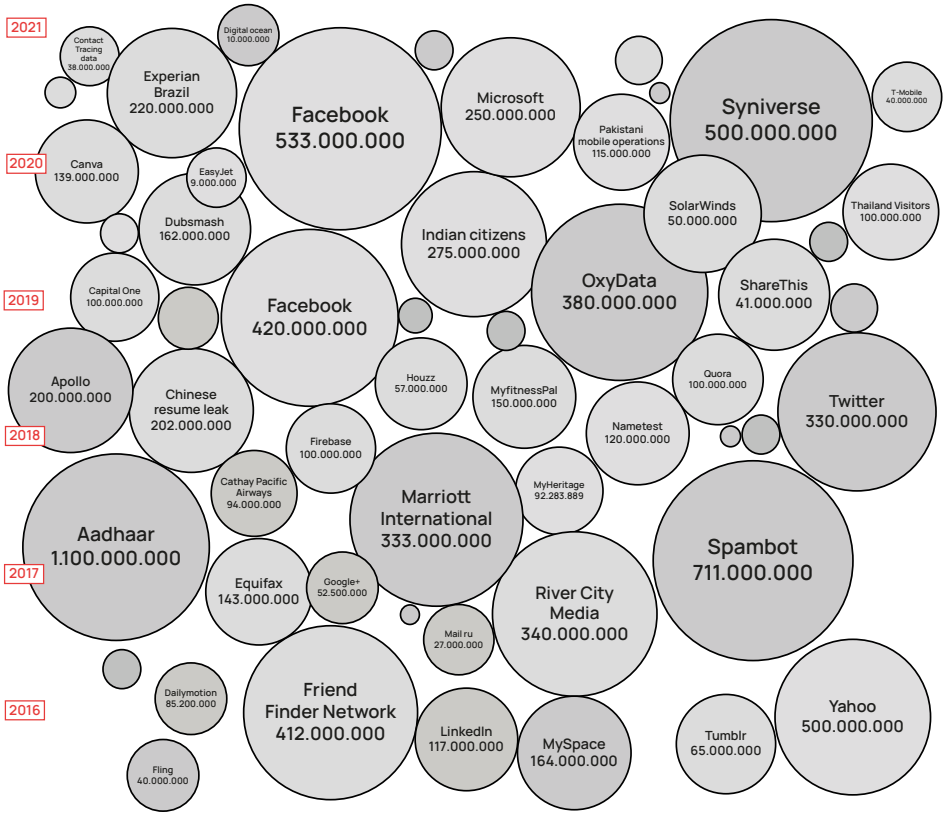
[4] https://www.ibm.com/security/data-breach

Despite being widely known that a data breach response plan backed by a risk management strategy is a proactive way to be prepared for such events, the vast majority of companies that handle user data or provide user services have neither. As such, user data continues to bleed into deep web markets, allowing for data abuse, fraud, scams and identity theft as a common occurrence. Increasingly, the average consumer internet user ultimately foots the bill, for the damage to their lives caused by the negligence of their service providers and data custodians.

The average cost of a data breach currently stands at just over $4.25 million USD, representing a significant vacuum for value across all industries. In addition to the high cost of data breach and threat mitigation, users of these networks often experience a compromise of their private data, wherein one data breach can result in a cascading leak of their personal information. And the scale of the problem cannot be understated: the 2017 Equifax hack compromised the private financial data of over half of the population of the United States.

Perhaps more ominously, earlier in 2021, the SolarWinds hack - which is still in the mitigation and damage control phase - saw the divulgence of state secrets and highly confidential government files, resulting in some of the world's largest transfers of wealth and IP in history.

Its cleanup is estimated at 100 Billion USD and will take years. Cyber experts agree that even after all that work is done, there will be no way to be sure the attackers have been successfully excluded from the currently infiltrated networks. The opaque digital warfare occurring around us at all times continues to impact the average user more intensely than anything humankind has historically experienced.[5]



Data Breaches by number of records lost[6]

[5] https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/

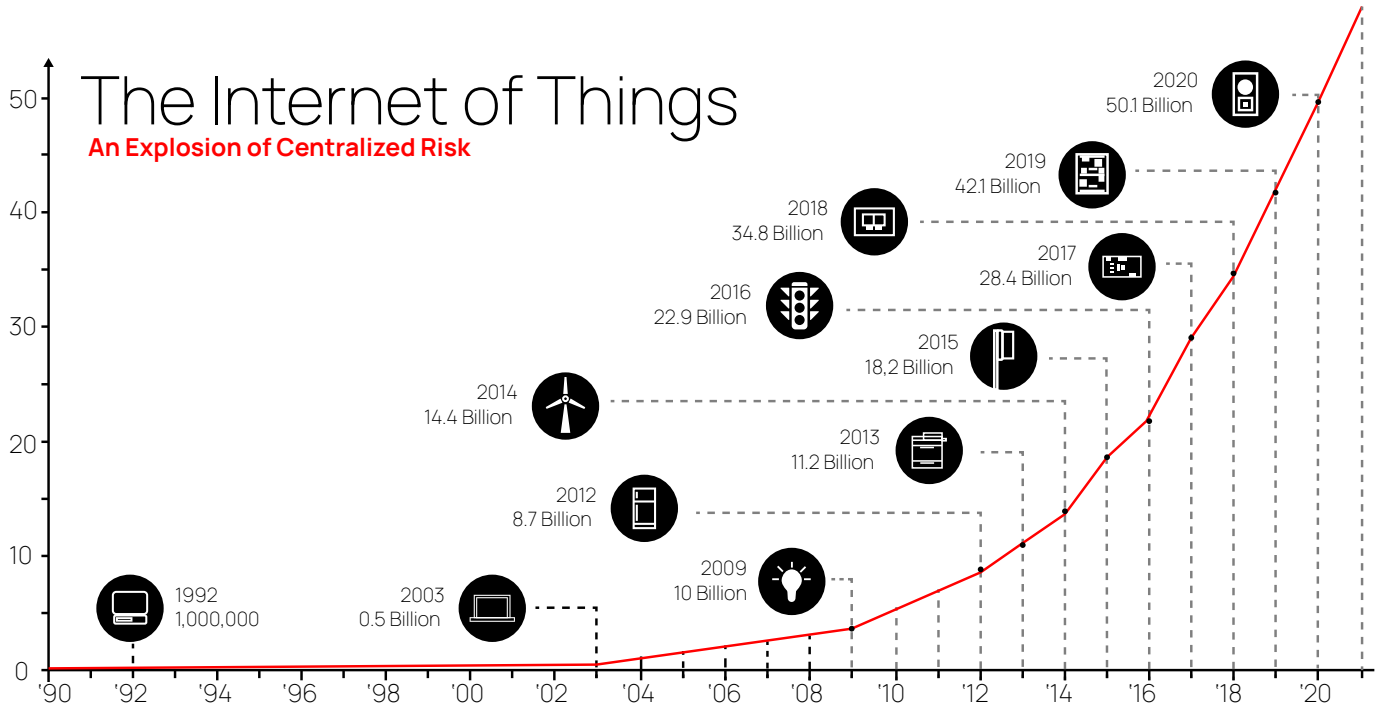
[6] https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Today, there are various risk-mitigating solutions to choose from, as mentioned above. These solutions, however, are not perfect, and rely on strategies that must be established to otherwise circumvent some vulnerabilities with this model, while keeping it clearly ahead of traditional technologies used in this space. As such, to achieve a design of a system that identifies deceptive inputs from malicious actors that own nodes or have subverted them in their workings, while discouraging such subversion activities, we suggest that the most important cyber platform of the current age will be the one that focuses on the way to pick the ideal model for the job at hand.

With this in mind, it requires the provision of a safe, performance-heavy and light-processing, elastic cyber-dedicated consensus mechanism, relying on multichain capabilities, whether for speed or resiliency, and for added risk-mitigation across trusted-nodes following a permissioned-defined list of rules of engagement. The consensus mechanics themselves may be paired using almost any technique of Sybil immunity to generate an openly, verifiably secure environment for such critical backbone data and metadata transactions. A Sybil attack is an attack in which the identities of the node are subverted and a large number of pseudonymous identities is produced to gain access to the network.

2.4. Current Perspective on Cyberspace

Today, it is evident from the degree to which it has become ubiquitous to use multiple devices across multiple networks, that such complexity passes mostly undetected in our own lives.
Thanks to mobility, traditional computers have evolved from mainframes to portable laptops, to powerful mobile phones, smart-watches, smart-cars, smart-refrigerators, smart-homes and tablets - all connected. Computers have experienced a massive change, from mainframes to very portable devices.



Exponential Growth overview of centralized devices globally over time

We end up dependent for most of our computing, work and play on the World Wide Web, the internet and other supporting mobile wireless networks. An incredible variety of kinds of hardware systems, architectures and networks are connected to form a worldwide cyberspace. The absolute penetration of networks and technology in contemporary society means that everyone and everything are to some level connected, even in the most remote of locations. It is unsurprising that we as a society and as users inevitably cease to fully comprehend the inter-connectivity of today's world due to its sheer complexity, and start to overlook its vast vulnerabilities and risks.

From an individual perspective, cyberspace is just a "platform" in society, as described previously. It is a fluid and constantly developing 'living system' or network, and also an environment that has so many things happening at once within it, that it is now far from governable. When it comes to governments' attempts to come up with effective policy, governance systems, compliance rules and laws to try to cut back on the ever-increasing number of cyber-attacks, these attempts are present and documented - but siloed and behind the curve of innovation, which can be demonstrated by the varied regulations and attempts at standardization - such as Data Privacy Shield, GDPR, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), National Institute of Standards and Technology (NIST), ISO/IEC 27000 standards family. As digital complexity grows, convergence and interoperability of these standards becomes less and less viable.

The sophistication and dangers originating from these varied phenomenon are not currently quantifiable, only estimates exist - since these are best-efforts led within specific time frames, within specific environments and concluded through limited intelligence and budgets, it will be indeed impossible to ever achieve truly global actionable consensus. Even though there is no international definition of network theory, a network is characterized by scholars as a "complicated pattern of connections among numerous interdependent elements".

Scholars of network theory recognize that since networks are complicated and centerless like the systems that make up cyberspace as we know it, deep levels of uncertainty are inevitable in generating, managing or planning security environments for complex networks. As will be discussed further on in this paper, despite the lack of feasibility in achieving full understanding of complex global networks and their weak points in federated organizations, a blockchain-based approach of 'divide and conquer through consensus' is possible (and indeed verifiable.)

When we take network theory and proceed to apply it within cyberspace, it becomes increasingly important from both a theoretical and practical standpoint. Cyberspace is a significantly networked environment, and as such, it's completely interdependent - because of its operational objectives and the nature of its services provided to organizations and consumers by organizations and consumers. It is, in essence, a worldwide network of programs in which fresh and varied technologies have been continually developed and deployed on a daily basis, and as is widely known - despite efforts to the contrary - there are vulnerabilities in these technologies and supporting frameworks that are known and unknown, unwillingly created, and discovered daily.

There is also no such thing as linear, expected inherent risk, danger or vulnerability of a cyber network or a protocol, software or otherwise any method, despite the wildly illogical current strategy that currently prevails in the space of opting for the 'proving the negative' tactic with expected current low probability results. **A completely different approach is suggested in this paper, with a dedicated distributed consensus of principles, dPoSec, placed on the control of risk, vulnerability, truth and trust in the digital context of our world.**

The context of such problems are best described with self-similarity theory through the dynamics which frequently are observed within study cases on such types of theories called the 'cascading dynamic events'.

The self-similarity concept in the context of networks and systems is a time-developing phenomenon that remains constant the more you zoom into the network. It is said to exhibit self-similarity if the numerical value of certain observable quantity of devices in this case {f(z,t)} f(z,t) measured at different times are different but the corresponding system criticality rules of devices irrelevant of their inner complexity at a given value of {z/t^{y}} {z/t^{y}} remains invariant.

This phenomenon seems to happen in networks if the quantity {f(z,t)}, f(z,t) exhibits dynamic scaling, just as in a fractal. The idea is just an extension of the idea of similarity of two networks in this case. Note that two networks are similar if the numerical values of their devices or systems are different, however the corresponding system criticality rules - such as the criticality of the applications on their devices - coincide with adjustments that can't fit into a linear paradigm.

A cascading event is a scenario in which, if ripples disperse across areas or sectors from the point of source, changes can be proven incrementally - in this case through an ecosystem of consensus given the right incentives. We let the various parts of the fractal network work do the right thing, being fully conscious of the truth of other fractal locations. We've established in the former paragraphs that many networks and systems don't normally function in a simple linear fashion, and have neither linear risks or vulnerabilities, but these same risks or vulnerabilities tend to create new risks either by repetition or by inheritance.

Within this case, once we employ the cascading event into some cyber-attack it efficiently transforms into a more dangerous and uncontrollable version of a multi-sector cyber-attack. This enables or permits the unsavory prospect of the destruction or harming of numerous critical sectors like critical infrastructure or government structures by focusing the cyber-assault in areas which might look to the unsuspecting observer as less crucial. This leaves any nation-state or critical infrastructure available to weaknesses that can be exploited due to weak implementation of security policies of a completely different allied nation-state, industry or sector (such as the Solarwinds hack of 2021 - 56% of cyber attacks occur through third parties.)

2.5. The Importance of Intelligence Backed Actions

> *Action may be the true way of measuring intelligence*[7].
>
> **Napoleon Hill**

intelligence noun (ABILITY)
[U] the ability to learn, understand, and make judgments or have opinions that are based on reason 7:
intelligence noun (SECRET INFORMATION)
[U, + sing/pl verb] secret information about the governments of other countries, especially enemy governments, or a group of people who collect and deal with this information:

Despite the general 'abuse' in the CyberSecurity space of the word 'intelligence', in this context we suggest using it as a means of source of knowledge, truth seeking, and judgment making based on reasoning that the blockchain ecosystem allows for such distributed proofs to be created and independently verified (intelligence noun, ABILITY.)

2.6 Value of Cyber Assurance

Modern society is dependent on the equilibrium of complicated infrastructure programs for virtually every economic and social purpose. The damage that can occur both from cyber-

[7] https://dictionary.cambridge.org/dictionary/english/intelligence

war type attacks to future cyber-terrorism is well known and accepted by nation-states and their agencies (US's Cyber Command, UK's Cyber Defense Force and Cyber Incident Response teams, among others) regarding the dangers and risks coming directly or indirectly from cyber-attacks, that could have a crippling impact on the country's economy, health, safety, and security, and social stability at large. The vital value of infrastructure is a consequence of developing lasting interconnectivity.

Likewise, individual business sectors within a connected economic model are inherently shaky, and disturbance in any single industry can activate a ripple through the economy, impacting businesses that indirectly and directly interact with the impacted sector.

Hypothetical Case Study. 1.
Within a nuclear power station, a group of critical PLC's and SCADA systems are attacked using the notorious Duqu malware. Its core is shutdown as quickly as possible to prevent damage, this creates issues with power and voltage levels in an aging electrical infrastructure - affecting hospitals, airports, dams, and even the stock market, creating unmanageable brownouts that end up heavily affecting the economy, and causing loss of life through a cascading event.

Hypothetical Case Study. 2.
Most banks use the SWIFT System, a federated semi-centralized system. If a SWIFT terminal is subverted by a nation state threat actor that is under a SWIFT system isolationist sanction, the cascading event would paralyze areas of the economy directly dependent on quick loans, that would in turn paralyze other more diverse sectors of business through a cascading event, hurting the reputation of the western banking system, weakening ongoing sanctions, making future deployments more difficult, and fostering the adoption of other, alternative banking systems, etc.

This shows the deep significance and importance of changing our perspective and understanding of cyberspace, from the traditional approach to a multidisciplinary or even a non-standard theoretical standpoint. Network theory, self-similarity concepts and the understanding and consensus needed around critical environments, and the negative energy unleashed by cascading events, contribute greatly to the field of cyber security and its solution-finding quest.

Theoretically and in the real world, it is crucial to comprehend the size of interconnectivity across the world. It is, by understanding a cyber-attack within a single sector or area which might not be deemed important but can have a massive effect on a country's safety/organizational capability, that we have the power to envisage and indeed project solutions into this important problem. This enables us to create better answers and new approaches based on the blockchain, that offer new techniques, never possible before in a robust manner that can deal with cyber-attacks now and in the future. By following new models and plans of defense through distributed systems, areas of business that are separated in principle can operate together in consensus. Additionally, it helps professionals within those organizations or structures to devise effective coverage to ensure the security and sustainability of their physical and virtual universe is maintained through control and verifiable unbiased visibility, across various cyber domains within their networks and outside of their environment.

3.0. New Design Principles for Reinventing Organizational Structures and Upgrading Society's Security Posture

3.1. Establishing Trust in Trustless IT Systems

Given today's rapidly growing CyberSecurity risks, the demand for a difficult-to-disrupt method to complement traditional CyberSecurity techniques is growing. The fact that spoofing, cyber-attacks and other types of disturbances seem to be growing in frequency and severity, makes the requirement to meet this need an all important one. Such abuses of currently existing infrastructure, architecture and protocols have the potential for catastrophic impacts on our own lives and global financial activity. In order to accomplish this need, Naoris offers to operate through a set of abstractions that greatly drop the risk of being compromised, along with a strategy that defines trust and reliability by a set of well proven methods that include zero-knowledge proof techniques under validators for verification of Merkle hash trees.

This situation ensures that attacks are mitigated even at the limit of a completely subverted corporate network, in which every verifier node is acting with malicious intent. Regardless of how many verifier nodes exist to be verified, the majority in comparison will always be chosen at random from the online network where the verification source is, thus the probability to guess and act to compromise any selected network apart from sizing are negligible.

Resilience is also added to the context of distributed truth finding operations, through enforcement of mandatory consensus of at least two high-tier trust-nodes. These nodes have much higher computing power and follow known cyber security standards in a verifiable manner, and as such can provide various operations over the hash tree and the source hashes.

From a reward perspective every validator node that is randomly chosen within a business, or other organization, receives bonus rewards for validating a breach or the submission of new intelligence data, or otherwise some compromise of the ruleset defined when compared to normal block rewards. Thus ensuring that the whole ecosystem's main focus is squarely on the task of finding malpractice or other malicious subversive activities.

Each client within a Verge Cluster is put under what is treated as an equally critical and optional setting, that can be optimised to define special privileges for each set of data. Additional privileged data containing blocks will result in allocating more rewards for the correct work.

3.1.1. Simplified and Resilient Approach to Risk

Arguably, in regards to security tools in general, sophistication is its own enemy, as so many alarms are generated through so many possible attack vectors that it becomes unmanageable. Organizations suffer higher costs through increased supporting staff, or supporting infrastructure, with the potential solution costing sometimes more than they gain through mitigated risks, from a cost management perspective or due to being overwhelmed with possible threats via third parties to manage their own security, which brings extra risks. Naoris suggests that it be leveraged to its fullest by organizations creating an ecosystem in which companies, organizations, or users DAO`s secure each other indirectly without the risk of loss of data or breach. By doing so or by using centralized solutions, Naoris becomes an evermore resilient and trustable super environment that does not transfer data but, their quantum-resistant one-way collision resistant hashes.

3.1.2. Parametric Bayesian Inferences and Modelled Consensus Secure Baselining

Arguably the domains of CyberSecurity experiencing huge transformation is endpoint security and AI backed solutions. Despite the constant advances in this domain to mitigate known threats, a lot is still needed in order to achieve truly mature-network-sized endpoint protection. We propose a succession of techniques, compared with the standard strategy. The objective is to predict and avert a wide array of risks are direct or as part of a cascading event.

The security of a certain network can directly be influenced by the importance of applications and the data used by a particular business process. The possibility that a change in the process or new application can be malicious, can be determined by several means. It can be by the user that made the change, portion of the change, timing of the change, rate of change per period of time, previous historical records on changes, circumstance of other running applications, and a number of other different activities. Thus, whenever there is information of a particular kind that needs to be processed in order to get an unambiguous conclusion based on probability or evaluation of the risk, Bayesian networks are a good choice in order to create whitelisting / blacklisting rules that are validated over time through consensus.

The Bayesian network's formalisation was devised in order to allow for an efficient representation of probability given a list of truths. The procedure enables a system to learn from experience, and it unites the areas of AI and neural networks.

In this context, Naoris enables the owner of a Verge Cluster, through the Naoris DApp for Command & Control (C&C) to set learning timers for different systems. An example can be given for a potential critical system, where the owner sets learning timers for an initial 30 days, where all applications that run there should be known and identified uniquely, all the libraries called should be known and identified uniquely, all the device drivers enabled should be known and identified uniquely, etc. These will all be part of a secure signature that is going to be collected by the sensor on the system and stored on the blockchain.

There are quite a few applications of such a technique, notably finding potential malware or otherwise unwarranted or untrusted software running alongside well known and expected applications, even a certain executable file that was known but suddenly has a different signature due to a code injection attack or the use on an unwarranted or subverted library, and even risky malwareless system actions like:

- running a command as superuser or root,
- connecting to the internet through an insecure protocol like SMB, RDP, FTP or an Anonymous socks5 Proxy among other examples.

After that Modelled Consensus Secure Baselining (MCSB) is defined and may be used as a parameter for Bayesian inferences made by the AI engine in a future disturbance of that same expected secure signature.

3.2 From Centralized to Decentralized

Decentralization isn't a new phenomenon. It was a part of the social structures of early human societies. They were small Neolithic decentralized communities of under 100 people in which everybody was responsible to and for one another. A smaller population size allowed this type of governance to be more streamlined. But later such small communities morphed into complicated and hierarchical societies dependent on centralized forms of government.

The concept of a ruler taking the lead and centralizing decision-making was suggested as a solution to the growing issues. The revolution led to increased production, and as communities became larger, it was impossible to keep a state of

overall peace without a central power to manage social interactions.

Centralization was initiated with the establishment of a central authority; the cost of production was ultimately decreased due to standard methods of production and trade, and improved production quality was also achieved and led to greater coordination within society.

The major benefit of using centralized systems was its efficiency. It is easier to make decisions when a system is centralized, and there are virtually no duplicate roles. Additionally, because of the centralization of authorities, society is able to become fairly steady, predictable and stable particularly in projects that require final and fast decisions to be made without great care for what the whole wants or needs or is best.

The flaws in centralization become apparent. One of the main drawbacks of centralization is the assumption that the top management/board/control-systems always have the best interests of the people or systems under their wing. As centralization systems grow they are often shown to experience a decline in their effectiveness. Another issue with centralization is censorship and lack of truth and transparency.

If unchecked centralized systems can result in an unbalanced exercise of control by a small group of elites. The crisis of trust that hit across the globe following the aftermath of 2008's financial meltdown has been explained as the result of the collapse of trustworthy institutions like banks and financial institutions. This was followed by other critical failures of centralization, such as the misuse of technology and information for monitoring, interference of centralized, often wealthy power structures for the benefit of the few, or biased decisions caused by being influenced by private funds or corporate giants or other large organizations of centralized power, etc.

This increasingly leads to a call for a possible solution to the loss of trust among traditional organizations, and to establish live intermediaries that add to the capability to reduce the requirement for trust between different individuals. This is why decentralization which delegates, validates and ensures fairness in decision-making and planning from central authorities is vital.

Distributed ledgers aren't new. They offer a secure solution for record keeping and accounting. DLT is a type of network of interconnected devices within a network with no central server that distributes information; instead, the networks of connected devices cooperate in order to create a consensus regarding sharing and storage of information. Because of the consensus protocol that all machines are in agreement with, when the information is recorded on the ledger system, it will be necessary to achieve, ideally, the consensus of all machines to allow for that information to be altered. This ensures the security of immutability, as well as the transparency of a trusted system.

Decentralization is vital to the progress of civilization. Additionally, decentralization through technologies like blockchain can result in the transparency of, and accountability in: finance, governance communications, CyberSecurity, auditing, enforcement of standards and other crucial tasks.

Sectors like supply chain management as well as property rights, contractual agreements, as well as digital identity, CyberSecurity, data assurance and trust are all areas that can greatly benefit from decentralized technology. In the end, it is very clear that blockchains will play a significant role in the good governance of global sustainability, as well as equitable economic development and the security of operations in all domains of digital technology, which are, obviously, backed by trust systems and security in digital form.

3.3. From Siloed to Interoperable

The CyberSecurity industry is facing an important issue that is markedly slowing progress towards improving security postures for businesses and organizations across the globe. It is about the dispersion of security operations within organizations. This can be due to a variety of reasons, such as the use of multiple diverse security tools, the lack of the management structures or absence of interconnected processes, etc. While the causes behind isolation of security operations could be different, all companies suffer the same negative effects and repercussions.

Security operations are composed of a variety of teams within an organization, each of which might use a different technique or stack of tools. In many instances, companies employ specialized tools to deal with specific scenarios. In the short-term the addition of a dedicated tool might appear like a sensible option however it only increases the workload for operations over the long run. With each tool, businesses must educate their employees and they may need to alter their process. It's not difficult to see the reasons why this isn't an effective strategy, particularly for CyberSecurity, due to the emergence of new threats and emerging security technologies evolving with the added complexity that devices on premise and on cloud, and now within unsafe networks of people working from home and their associated risks - such CyberSecurity structures are not made to work across networks and do not support today's decentralized workforce mentality, in other words we`re using centralized solutions in a decentralized world.

It's quite difficult technically and operationally to determine the exact amount of equipment employed in security operations because it's a sensitive issue that could compromise the security of the company. Many of them are siloed both in their management and operations, so it's not unusual that these tools themselves are a source of risk towards the organization as discussed in other locations of this whitepaper. However, a number of industry studies and reports have shed the spotlight in recent times. A survey conducted in 2017 conducted by Enterprise Strategy Group (ESG) found that 40% of 412 respondents utilized between 10 to 25 safety tools. In addition 33% of those surveyed utilized between 26 and 50 security tools. A 2017 study in the field of financial services from market research organization Ovum discovered that over 73 percent of respondents used more than 25 security tools in their security processes. The majority of the organizations that were surveyed had more than 100 security tools. All these tools are siloed and do not talk to each other, they are in most cases black boxes themselves that can insert risk into the organizations, but barring a decentralized solution, they are "the only" option.

Gartner identifies in its 2022 Tech Trends the CyberSecurity mesh as one of the core technologies the majority of the world's organizations will be using in the next few years.
Gartner analyst Felix Gaehtgens said the CyberSecurity mesh approach is a strategy rather than a structure. However, the idea improves the alignment of organizations and the threats they face: "Attackers don't think in isolation. They think in silos," he noted.

Naoris suggests that businesses or users in centralized or decentralized organizations should have an alternative that empowers them with the layers of trust and support needed to deliver the essential security mesh strategy required in a naturally decentralized way that benefits from decentralization instead of seeing it as a risk. While being by its own nature, orders of magnitude more resilient than centralized siloed tools, and not vulnerable to black box stemming attacks like supply chain attacks and breaches of trust, a decentralized CyberSecurity mesh approach that is owned by themselves is desirable and preferred, as there is no need to transfer risk to any third parties. The CyberSecurity mesh naturally embraces the defense in depth principle and suggests that all

needed centralized “traditional” cyber tools should still be used in conjunction and within the mesh that secures environments and assures the tools themselves are not compromised.

This includes identity fabric, security analytics as well as policy management and useful dashboards. Interoperability and distributed security will be the main ingredient in creating and implementing a security mesh. This will certainly change how CyberSecurity is thought about and delivered.

3.4. From Proprietary to Open

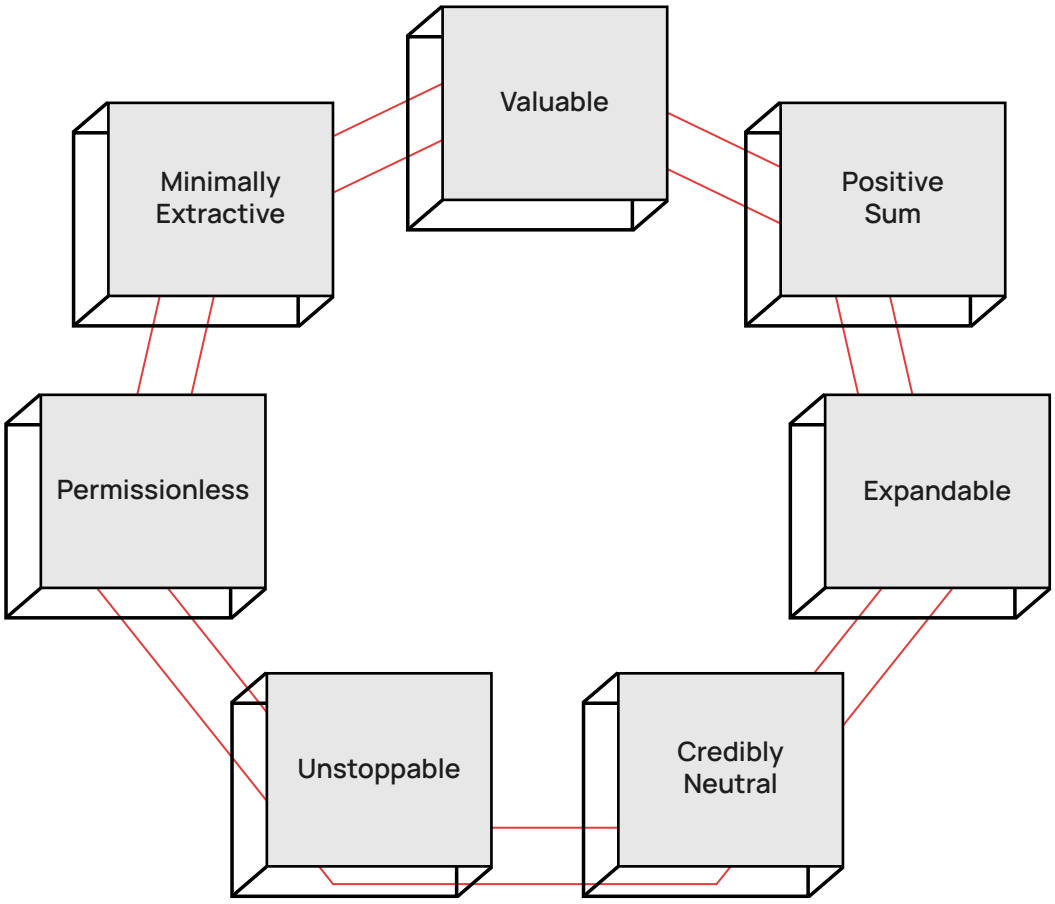
A rapidly emerging trend noticed by companies is the trend of trying to know the basic advantages and disadvantages of implementing open-source-based tools and how they’ll impact their CyberSecurity plans. The rise of a number of open-source IoT platforms such as DeviceHive, Macchina, Eclipse IoT and ThingSpeak as well as many others and an array of open-source stacks, companies are unsure of the security and protection against risks in open-source applications.

Although open source makes code available, it’s observed that visibility of sources is not enough to reduce the security risks that are posed to an individual project in the majority of cases. Security experts report that in certain situations the visibility of source code can help to bring projects to secure and stable conditions.

Naoris, as one of the contributors to open source, strongly believes that open source code doesn’t create any significant obstacles to security. Instead, it enhances the security of code by involving a wide range of users with the capability to report bugs swiftly providing customers and the general public at large with tangible examples of reusable, reliable, refactorable and as a consequence of scrutiny, secure code.

	Proprietary	Open Source	Decentralization
Code Base	Closed	Open	Open
Decision Making	Opaque	Large Oversight	Large Oversight, Many Actors and No Single Point of Failure
Community	Private	Open	Open and Scalable

4.0. HyperStructure



Following the Ethos: Attributes of The Naoris Protocol HyperStructure

4.1 The Need for Adopting the HyperStructure Ethos

Escalating planetary scale cyber threats demand a new set of design principles. Traditionally framed companies are subject to various attacks that stem from abuse of power, censorship, and bribery, to name a few. To address these risks and many others, single points of failure need to be eliminated from the picture for a long term solution to emerge.

In short, the digital infrastructure that is required to address CyberSecurity issues in the 21st Century needs to outlive its founders, the company that started building it and the attacks that various actors interested in tampering with such an important infrastructure will attempt.

The traditional definition of infrastructure is “the basic physical and organizational structures and facilities (e.g. buildings, roads, power grids) needed for the operation of a society or enterprise”. Clearly, a digital world requires digital infrastructure. And as we have learned, digital infrastructure such as Social Media and News platforms, which are owned by centralized entities, may be great business models for the moguls running it, but are not in the best interest of the general public. Decentralized models point to a better path.

A CyberSecurity mesh that is engineered to enable every device to protect each other needs to go beyond being a digital infrastructure - it has to be antifragile, becoming stronger the more it is attacked - and designed to serve everyone, without prejudice, for generations to come, if not forever.
For a Decentralized CyberSecurity Mesh to become the massively adopted protocol that finally is able to turn billions of untrusted devices into the most secure network of networks that the world has ever seen, a paradigm shift is required. Therefore, we're not just building a protocol. **We're building a HyperStructure.**

A DAO (Decentralized Autonomous Organization) governed protocol via quadratic voting may be an important initial step towards effectively maintaining a planetary scale for-public CyberSecurity infrastructure, but to build something that becomes mission critical for realizing the future we believe we all deserve, new, bold design principles should be adopted. We can't do the same things over and over and expect different results.

Before we outline and describe the attributes that make a protocol a HyperStructure, it is important to note that although all HyperStructures are protocols, not all protocols are HyperStructures.

Another point worth mentioning is that at the time of this writing (January 2022), HyperStructures are more a Concept than a Thing. This means that as more protocols are built according to a HyperStructure Ethos, definitions may change slightly and new attributes may prove to be as important or more important than the ones explored below.

What we currently know for a fact is that building a HyperStructure is more than desirable for building the foundations of the new internet. HyperStructures may actually be the only way to build truly important digital infrastructures that are capture resistant and allow the dreams and work of builders to come into fruition without going spoiled shortly after, while benefiting the many, not the few.

In the Digital Age, CyberSecurity, like Privacy, needs to become a basic human right.

4.2. The Attributes of a HyperStructure:

1. Unstoppable
2. Permissionless
3. Minimally extractive
4. Valuable
5. Expandable
6. Credibly neutral
7. Net positive.

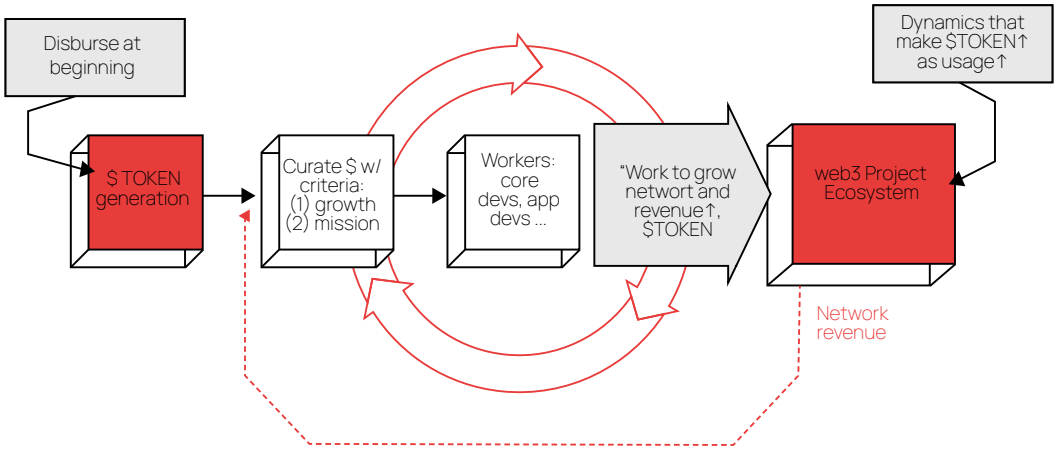
- **Unstoppable:** Protocols that are unstoppable are built to run indefinitely, without degrading. No one should be able to stop such a protocol. Not even power structures or the creators of the protocol itself. HyperStructures should be multichain, else they are subject to the longevity of the blockchain in which the protocol runs. HyperStructures' smart contracts and mission critical files should be hosted on the permaweb, meaning that they should remain online indefinitely, come rain or come shine. Devices and networks can adopt it or abandon it, but one of the main attributes of a HyperStructure is that it can't be stopped. The off switch does not exist, so even a DAO wide vote would not be able to turn it off, removing another attack vector of the CyberSecurity Mesh.

- **Permissionless:** Approval by a trusted authority is not required to join the network and any user who wishes can participate in the protocol. All devices who become part of the CyberSecurity Mesh become validators of the state of the network and the same level of security is presented to everyone. Users and builders cannot be deplataformed. HyperStructures need to be censorship resistant and accessible by anyone.

- **Minimally Extractive:** We defend that HyperStructures need to be minimally extractive - which means, a protocol should charge near base cost fees to incentivize adoption, and disincentivize forking, while ensuring that the ecosystem development treasury is managed by the DAO remains robust to allow a strong ecosystem to emerge. While Naoris Protocol has a clear vision of what its core should be, being able to adapt and evolve the CyberSecurity Mesh and the ecosystem around it is critical for its longevity and effectiveness against cyber threats.

- **Valuable:** The protocol is conceived to be a for-public endeavour, and yet, extremely valuable to own and govern, which sparks an ecosystem around it. If a protocol is not useful for its users, it has no reason to be adopted, and stay relevant for the long term. If owning and governing a protocol does not provide any benefit to its governors, it becomes hard to maintain. Altruistic actors may exist, but they are not common. The challenge is to strike a balance between accessibility for all and value for the ones governing the protocol. The larger the Mesh becomes, the more valuable it becomes. In a tokenized machine economy with a capped token supply, it's natural to imagine that the more valuable the mesh becomes, the more valuable the underlying tokens responsible for the security handshakes will be. Naoris Protocol derives its value not from Total Value Locked (TVL), but rather from Total Value Secured (TVS). The more valuable networks join the CyberSecurity mesh, the more valuable the protocol becomes.

- **Expansive:** Powering potentially hundreds of billions of security validations per day, the protocol needs to possess built-in incentives for users to behave fairly and for builders to continue iterating on the protocol and building on top of it at the application level. Most well funded blockchain protocols are able to set up an ecosystem development grants program, but how many can continue to foster the ecosystem in the years to come? For the longevity of grants programs to increase, a positive feedback loop is required. A portion of the minimally extractive fees generated by a growing number of participating devices needs to be directed towards a dedicated treasury for ecosystem grants, which is known as a Web3 sustainability loop. For the long term success of a HyperStructure, there should be incentives for entrepreneurs to continue working on defending the mesh against new threats. CyberSecurity is a dynamic realm and thinking that this nature will change would be both dangerous and foolish.



The Web3 Sustainability Loop Model, as proposed by Dr. Trent McConaghy, Co-founder @ Ocean Protocol.

- **Positive Sum:** Wide adoption and usage of the protocol results in a win-win environment for all network participants. This happens at all levels of the protocol. As more devices of a network use the CyberSecurity Mesh, they become safer for all participants of the network. As more networks of networks participate on verge clusters, entire economic sectors subject to the same compliance standards become more secure, with verge cluster-wide learnings as attacks on any devices belonging to a network inside of a verge cluster are attempted. The net value for society at large is access to security that aims to cost an order of magnitude less than current CyberSecurity stacks, while bringing detection and mitigation capabilities one order of magnitude higher. On a technology development level, the minimally extractive fees power an ecosystem development grants program, giving the community a clear path forward and blossoming a growing number of projects maintaining and building on top of the Naoris Protocol. Providing competitive participants an opportunity to collaborate on certain levels, using the same infrastructure for the benefit of all provides further elements for a positive sum environment.

- **Credibly Neutral:** To be adopted by a wide range of governments, companies and individuals, which are known to have different priorities and objectives, HyperStructures need to be credibly neutral. They need to treat everyone fairly and provide the same level of access and service to all users, to the extent that it's possible to treat people fairly in a world where everyone's capabilities and needs are so different (Buterin, 2020).

4.3. The Likely Outcome from Adopting the HyperStructure Ethos

Our belief is that the attributes of a HyperStructure are not just powerful on their own - they are highly synergistic. Building an important piece of digital infrastructure for Web2, Web3 and securing potentially all of the devices in the world with a peer-to-peer blockchain enabled CyberSecurity Mesh is an endeavour that requires thoughtful planning and design principles.

Once built on such an Ethos, a protocol becomes a for-public infrastructure optimized for massive adoption and its network effects, while actually solving the underlying challenges for which the protocol was designed to present solutions for.

Building the first HyperStructures is a privilege that our generation can enjoy as technological breakthroughs in the realm of blockchain scaling and decentralized governance converge with a new global value system that unfolds new possibilities for everyone.

As the transition from Web2 to Web3 accelerates, with powerful crypto economic incentives at its core, new autonomous and self actualizing structures for the world can be imagined, and one day we hope that future generations can look back into this point in time and marvel, acknowledging the advantages brought forward by the trailblazers and pioneers who ventured into a new world that is more equitable, resilient and adaptable to the new conditions of the ever expanding digital paradigm.

5.0. Technology Backdrop and the Case for a New dPoSec Consensus Mechanism

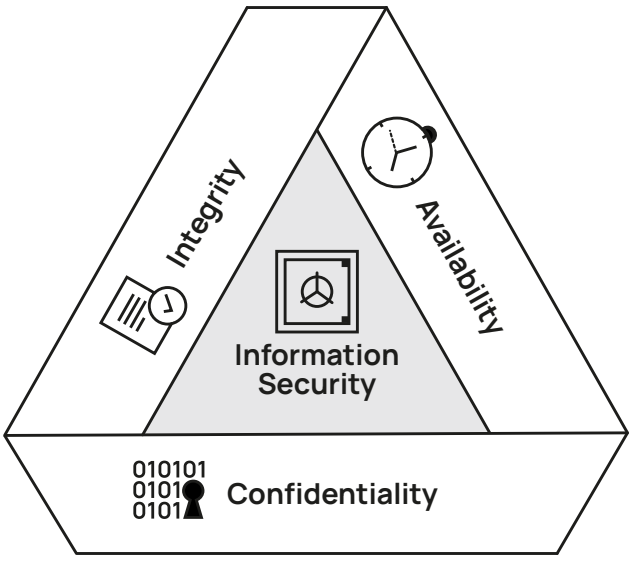
5.1. The CyberSecurity CIA Triad - Confidentiality, Integrity and Availability of Data

The idea of the CIA triad was created over time and does not originate from a single source.

Confidentiality was first proposed in 1976 through a study of an organization called by the U.S. Air Force.

The concept of Integrity was discussed in an article in 1987 titled "A Comparative Study with Commercial as well as Military Computer Security Policies" composed by David Wilson and David Clark. The paper acknowledged that computing in commercial settings had an obligation to keep accurate accounting records and correct data.

While it's not as simple to locate the original source, the notion of Availability was made popular in 1988. In 1998 the public was introduced to the three concepts as a whole, known as the CIA triad.



In the context of CyberSecurity it is necessary to examine the CIA triad as a model to develop CyberSecurity architectures. These core security principles guide CyberSecurity policies, however they aren't the only ones; Naoris's Protocol seeks to offer a hyper-resilient cyber security mesh that encompasses these core principles of CyberSecurity and more.

These core principles apply to ecosystems of any kind and magnitude, and must be taken into account to decisively mitigate the risk that occurs at the baseline level. Stemming from a myriad of threat methods that include breaches of trust and the tampering or subversion of trusted systems and processes. Naoris Protocol is governed by a Distributed Proof of Security Consensus (dPoSec) model that enables the environment to focus on growth and wider adoption by mitigating internal risks as well as validating other spaces for risks and threats. This creates a positive-sum decentralized effect in true HyperStructure fashion, providing a win-win position for the Web3 community at large with a permissionless and wholly beneficial approach that is credible and credibly neutral.

Confidentiality, Integrity and Availability referred to as the CIA triad is a framework developed to help organizations establish appropriate policies that manage the way they deal with security and information.
The aim for the triad framework is to guarantee that data is stored correctly and in a consistent manner, until changes are authorized by an authenticated authority or participant whenever they choose.

Data must be protected from disclosure due to the nature of the information that the organization is responsible for creating, processing and storing.

Confidentiality refers to the capability not to divulge information to unauthorized persons, programs or processes. Confidentiality is related

to the security of information as it requires the control of access to that information, and includes the capability to obtain or unencrypt such information through access control methods. It is essential to make sure that only authorized individuals are able to access information and that unauthorized individuals are not. In simple terms, confidentiality implies that something is kept secret and shouldn't be divulged unintentionally to individuals or organizations.

When confidentiality has been compromised it could lead to loss of privacy or disclosure of confidential information, IP, or the critical leakage of data to others or the general public.
There are many kinds of information that can be considered confidential, for example financial details, health records or other sensitive information like cryptographic keys or passwords. Certain types of information are more critical than others and therefore require a greater level of security. Implementations of such security methods within information systems are Access Level Restrictions (ACLs), used within cryptographic algorithms for data in transit or at rest.

Integrity refers to the protection against the destruction and/or modification of data, assuring that the information is not altered in an undetected way, as well as ensuring that the integrity of the information is maintained and it can be trusted and has not been tampered with. This applies to data as well as files, processes and even whole systems. This means that a cyber security threat or vulnerability to specific cyber attacks can be assessed by compromising any of the fundamentals. Integrity is founded upon encryption and hashing or hashing only, in order to provide the highest level of security against tampering and subversion, as well as cyber-related threats like cyber-espionage or sabotage of critical processes or data.

Availability or accessibility ensures that information is accessible to all who need it, when they need it, which includes prompt access capabilities, remote or local as needed, no matter the time of day, the place of residence, geographical location or any other factor. Outages or DDOS attacks are examples of availability failures.

The completeness and accuracy of data is essential for the success of any organization, ecosystem or entity, centralized or decentralized. The reliability and authenticity of data, processes and other operational assets are fundamental and critical, to ensure they are not susceptible to manipulation.

It is important to note that integrity is essential in order to safeguard data when it is being used, not just for the operational capability of any ecosystem, but also when used by others and by trusted third parties of that ecosystem.

The CIA triad should be held to the highest regard from an architecture perspective and validated through the highest trusted methods possible, the Security Goals of the RMIAS Model enhances the Triad and focuses on 8 goals that are considered key for a best in class baseline security level.

The CIA Triad:
- Confidentiality
- Integrity
- Accessibility/Availability

Plus the supporting 5 Security Goals, RMIS:
- Accountability
- Privacy
- Trustworthiness and Authenticity
- Non-Repudiation
- Auditability

The rapid adoption of innovations stemming from Blockchain 1.0 to Blockchain 2.0 and Blockchain 3.0 have an implicit promise offering bold claims of censorship resistance and unprecedented flexibility, however as much of this beloved technology, if not all, still rests firmly on real-

world critical digital services and networked systems that make up Web2 architecture.

We at Naoris present this as a serious intrinsic baseline threat, and a false sense of security for Web 3.0 applications that end up inheriting the risk of Web 2.0 systems. Naoris believes that safeguarding Web 3.0 using Web 2.0 solutions, if any, defeats the overall purpose of bringing services under the most trusted platform in the world. Naoris proposes a solution that can grow in parallel with other innovations to achieve the best that Web 3.0 can offer.

As such the Naoris Hyperstructure oversees a wholesome and positive-sum use case for all Web2 and Web3 participants that care about the quality of their CyberSecurity and service, while benefiting the whole community with their participation.

5.2. The Blockchain Trilemma and the Naoris Approach to Mitigating Risk.

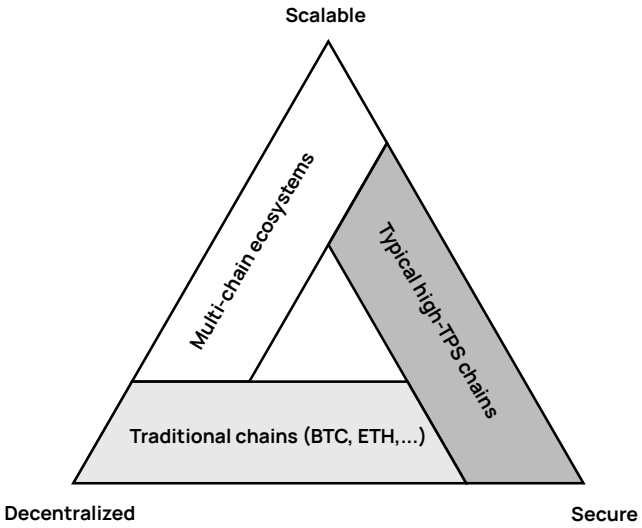
In regards to the Blockchain Trilemma it can be said that Blockchains are fundamentally connected by an absolute truth that is focused on three vectors, they are, Security, Scalability, and Decentralization. It is because of the decentralized nature of blockchain systems, that certain requirements were defined as fundamental to its workings. Since the inception of blockchains, a constant communication stream between all participants was deemed as paramount.

There are numerous ways we can define a distributed system. For instance the way in which it exists, in the most simple form, in one single computer. The central unit of control, the bus unit, the input output channel, and memory units are independent components that collaborate via distribution.

Satoshi achieved a breakthrough in the field of distribution by offering definitions resolving immediate issues and omitting intermediaries. The promoted perspective offers an alternative approach towards distribution studies that result in the development of many new protocols that have led to a number of breakthroughs. We should not forget that this distribution technique uses a consensus approach that was released a decade ago, after which you can find an entirely new collection of protocols which are being developed to surpass the Nakamoto definition, maintaining the original baseline ethos while at the same time using the former as a launchpad for improving and innovating around it, with the aim of creating a better world.

Consensus and its own efficiency have been the major areas of focus since the start of computing, with every up-to-date improvement, we are closer to solving the key questions and problems like never before.

In order to achieve an agreement or consensus on what will happen to the blockchain on each cycle, all participants, be it block producers, validators or other kinds of participants need to have the most current information to process.



This is referred to as synchronicity and is generally a limitation in decentralized networks, which requires extra potential time to spread information throughout the network to all participants.

Security refers to the resiliency of the blockchain against attacks at the protocol level, as well as the ability to change the blocks' data, which is also known as its source of truth.

Scalability generally refers to the amount of transactions, users and protocols that the blockchain can support without slowing or increasing transaction fees. It is often utilized in conjunction with the term "throughput" also known as "transactions every second" that a specific blockchain can permit.

Decentralization refers to how well-organized nodes, governance, and ownership of tokens or pieces of data or smart contracts are distributed across the blockchain ecosystem. Blockchains depend on a network of worldwide distributed nodes to achieve consensus which is basically an agreement about the type of modifications or changes the blockchain could undergo.

A decentralized network requires more time to achieve consensus across all nodes as compared to a single central node. This is why decentralization is fundamentally in opposition to scalability. Additionally the scalability factor is directly related to the security of blockchain. This is due to the fact that a small network is susceptible to being targeted and could have its irreparable blockchain information compromised, while an extensive network is costly to be disrupted.

Naoris Protocol argues that while these are important topics, just like for any other system type, distributed or not, the overall integrity and availability of the system has to be in working order under the CIA Triad and the RMIAS - Reference Model of Information Assurance & Security Model (an extended version of the encompassing triad) and other well known security standards. These standards constitute the basis of good security architecture by design, ensuing trust at the baseline level and mitigating risk to its operations. This is true for blockchain systems and supporting environments, like wallets, miners, exchanges, bridges and L2 Protocols.

Naoris Protocol's security is firmly rooted not only in its ability to process data in a scalable, decentralized and secure way, as validated by the Web3 protocol in question, but also its capability to be resilient against a plethora of threats and cascading risk events.

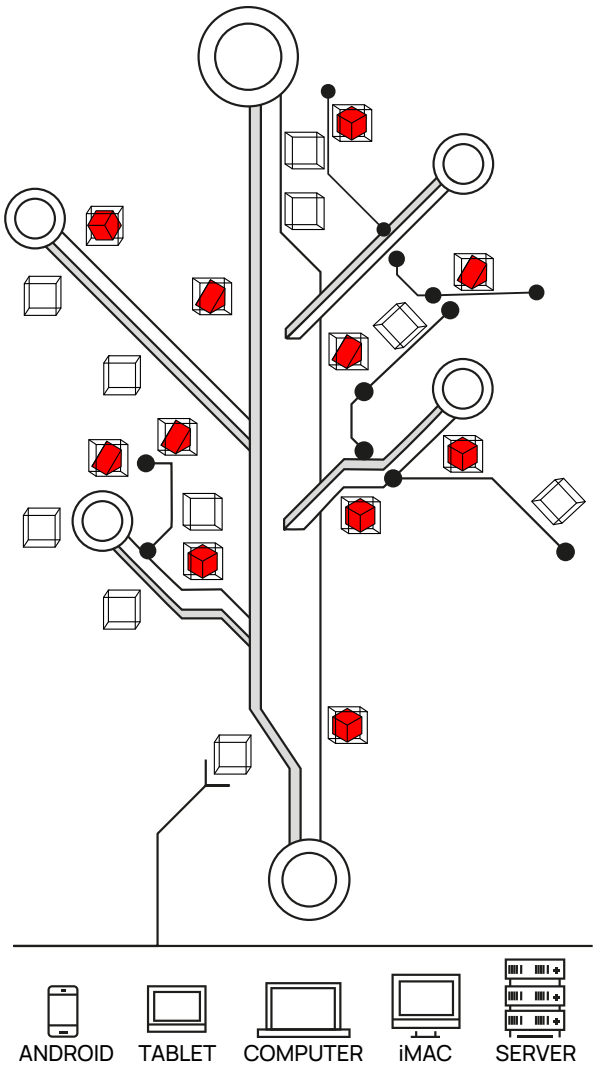
Events that are currently not managed from a decentralized perspective if managed at all. For example, Noaris must extend its resiliency to cover a more risky, single-point of failure or centralized perspective that uses opaque black box vendors for traditional security.

Vendors that operate without any enforcement, validation or mitigation efforts for any baseline server, process, access control management system, integrity, trust, patch level, known threat or service risk being enforced or validated before any data is submitted or validated by a node. This will lead to potential attacks of various criticality levels against the availability of the system and its security and trust and overall survivability and resilience.

Blockchains, supporting infrastructures and other DLT systems, just like any other system based on real world infrastructure stacks, Operating Systems and various layers of complexity across the OSI Model, have risks that are not only aligned with Web2 centralized environment weaknesses, but inherent to their nature, such as but not limited to:

- Account Hijacking risks at node, user and exchange levels,
- API tampering risks,
- DOS/DDOS,

- Consensus attacks, direct and side-channel against miners/block-producers, sidechains or shards,
- Data corruption or tampering of oracles,
- Wallet Vulnerabilities, tampering, code injection attacks, others,
- Internal threats in exchanges, oracles, protocols, bridges,
- Update poisoning,
- Code injection attacks, cryptojacking, namely malware in miners or validators,
- Advanced Persistent Threat risks,
- Sniffing attacks, Keylogging attacks against wallets and servers of any kind,
- Evil maid attack through hardware or firmware tampering,
- Identity and Access Management vulnerabilities on nodes, users, oracles, bridges, servers,
- Malicious browser extensions.
- Service provider attacks on oracles, nodes, users,
- Cascading events started by any of the above that trigger serious risks such as but not limited to survivability events or 51% attacks, among others.



A representation of node structures and device types

Current insights are pretty much limited to blockchain submissions, i.e the time of block submission, number of transactions within blocks, contracts responsible for the block creation and timestamps etc.

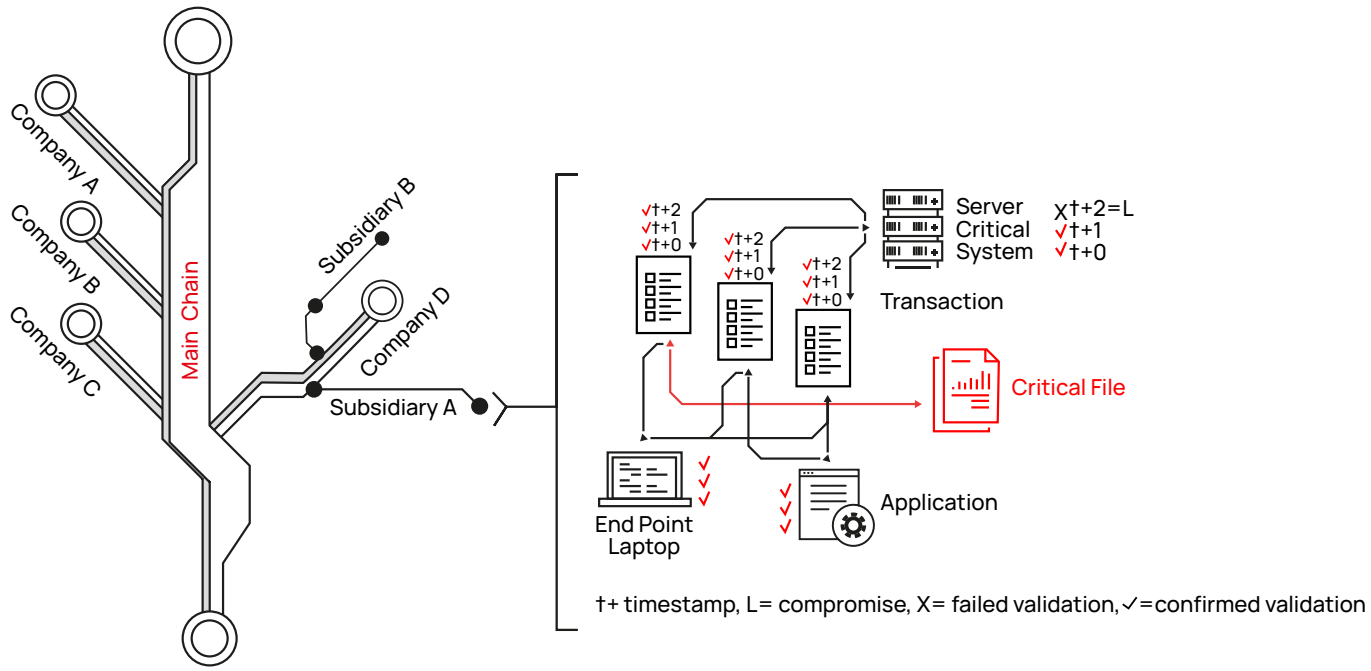
The Naoris approach aims to help support such environments without any impact to their operations, using its own dPoSec consensus mechanism which is focused on leveraging a higher trust and security level for these spaces which operate within their own private VergeClusters with their own rules and use cases, while needing no further requirements for changes to their operations or consensus model and leveraging their already existing infrastructure to their own defense.

The environments devices and services validate each other under consensual rules, ensuring mutual trust between themselves and ensuring the security and integrity of their services increasing their value and bottom line and the trust of processes and operations they have running.

6.0. The Naoris Protocol's CyberSecurity Mesh HyperStructure Framework

6.1. Ecosystem Overview

In the context of the world's ever growing inter-connected digital systems, our privacy, security and safety depend heavily upon the accuracy and validity of critical information generated by processes that traverse networks or rest within systems. Various innovations have been designed to eliminate the need for loosely-secured entities that control the flow of critical data, cryptographic keys and other logical assets, but each of these efforts has, in the best of cases, relied completely on a human-based centralized management model. A model where all systems and their surrounding infrastructure - be it, software or hardware based centralized governance structures, require human input and oversight to operate. Considerable efforts have been made to strengthen the overall state of security and trust of such centralized entities, all with the intention of making the internet a safer place, but after many years and many innovations, the current cyber threat is rising at such a pace, that no centralized solution can keep up with it. This has resulted in an exponential increase of risk to the globalized structures that support the world we live in.



dPoSec and Naoris CyberSecurity Mesh validation over time representation over a node and its processes

With years of experience in the field of critical CyberSecurity and risk mitigation, the team at Naoris Protocol have created a disruptive and contrarian design pattern that makes networks safer as they grow, not weaker. By turning any device, by its nature a centralized point of risk, into a trusted node and validator of trust, operating within a Verge Cluster and governed by a distributed assurance consensus, through this approach, the Naoris Protocol is bringing decentralization into centralized environments.

Inherent centralized risks are mitigated by leveraging the existing complexity, both in number of devices and also across disparate traditional networks, which to their own advantage, all operate under a distributed dPoSec consensus while at the same time acting as a resilience and trust assurance shield for other peers across the network.

The aim to decentralize CyberSecurity through a mesh HyperStructure enabling a generalization of trust at the baseline level is key in providing value to governance structures, enterprise, and the entire Web2/Web3 technology stack.

In this section we will provide an overview of the Naoris Protocol - a pioneering innovation in distributed CyberSecurity.

Naoris Protocol allows for pseudo-partitioning in a shard-like manner, such that the entire state of the network is distributed and maintained in partitions known as Verge Clusters.

Naoris Protocol supports both on-chain and off-chain sharding, where nesting Verge Clusters are deployed to serve independent business needs, embedded with case specific security and compliance logic to deliver precise CyberSecurity requirements. Off-chain networks can be optimised to act like an on-chain solution, making any organization or individual unstoppable even in the absence of any appropriate consensus.

The Naoris Protocol Design Principles are:

1. Enhancing scalability while ensuring security and decentralization
2. Protecting data in multiple layers instead of implementing single layer security
3. To only rely and work with trusted nodes
4. Keep close track and check upon vulnerabilities and act with ‘keep learning’ and ‘keep patching’ gaps
5. In-built capabilities to provide first layer Defense for all applications deployed on the network. For example, to auto check smart contracts for vulnerability attacks
6. Adaptability to preserve privacy
7. Off-chain can remain unstoppable
8. Open standard to support various Dapps
9. Incentive-driven ecosystem

Naoris Protocol provides an extensive interactive explorer that offers enhanced transparency to its users and Verge Cluster owners with access control and management capabilities for onboarded assets. This provides insights gleaned from the multiple rules that network specific security policies are based upon. These insights help keep a distributed validation track of compliance, cyber best practice, patch-levels, internationally accepted CyberSecurity standards like Health Insurance Portability and Accountability Act of 1996 (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), National Institute of Standards and Technology (NIST), ISO/IEC 27000 standards family among others, and even secure baselines that are under management to control the specific participation of a Verge Cluster domain, this is especially useful when third parties need to validate or audit SLA`s or compliance rules of subordinate organizations, i.e., Banking Sector, Critical Infrastructure sector and their third parties or National Regulators/Central Banks, etc.

Further Web3 related extensions include; reward viewer, status viewer, scheduler, CLI and SDK, ready-to-integrate templates, cross-chain barter system, and cold and hot wallets.

6.2. The Topography of the Decentralized CyberSecurity Mesh

6.2.1. Blockchain Topography Overview

In general blockchain can be divided into 4 layers:

1. **The Network Layer**
   The network layer provides network services and representations of data. Data representation is responsible for the storage as well as encryption and security of data. Services for network connectivity are accountable for identifying and communications with protocol peers, as well as routing, addressing, and name services. These are service providers, which includes those who control DNS names and IP addresses.

2. **The Consensus Layer**
   It is accountable for the rules to be followed by a sequence of transactions. It is classified into different categories according to the protocol type:

   1. Byzantine Fault Tolerant
   2. Proof of Work, as well as
   3. Protocols for proof-of-stake

3. **The Replicated State Layer**
   It is the replicated state machine component, which is concerned in the understanding and updating of the blockchain's status, is responsible for the task of processing transactions. This layer classifies transactions into two categories.

   a. The first is about the privacy of transactions as well as the privacy of those who created them.

   b. The second section is smart contracts. It is concerned with safety and security aspects of decentralized execution of code within an environment.

4. **The Application Layer**
   It is the most commonly used user-facing function. This layer can be divided into 2 groups.

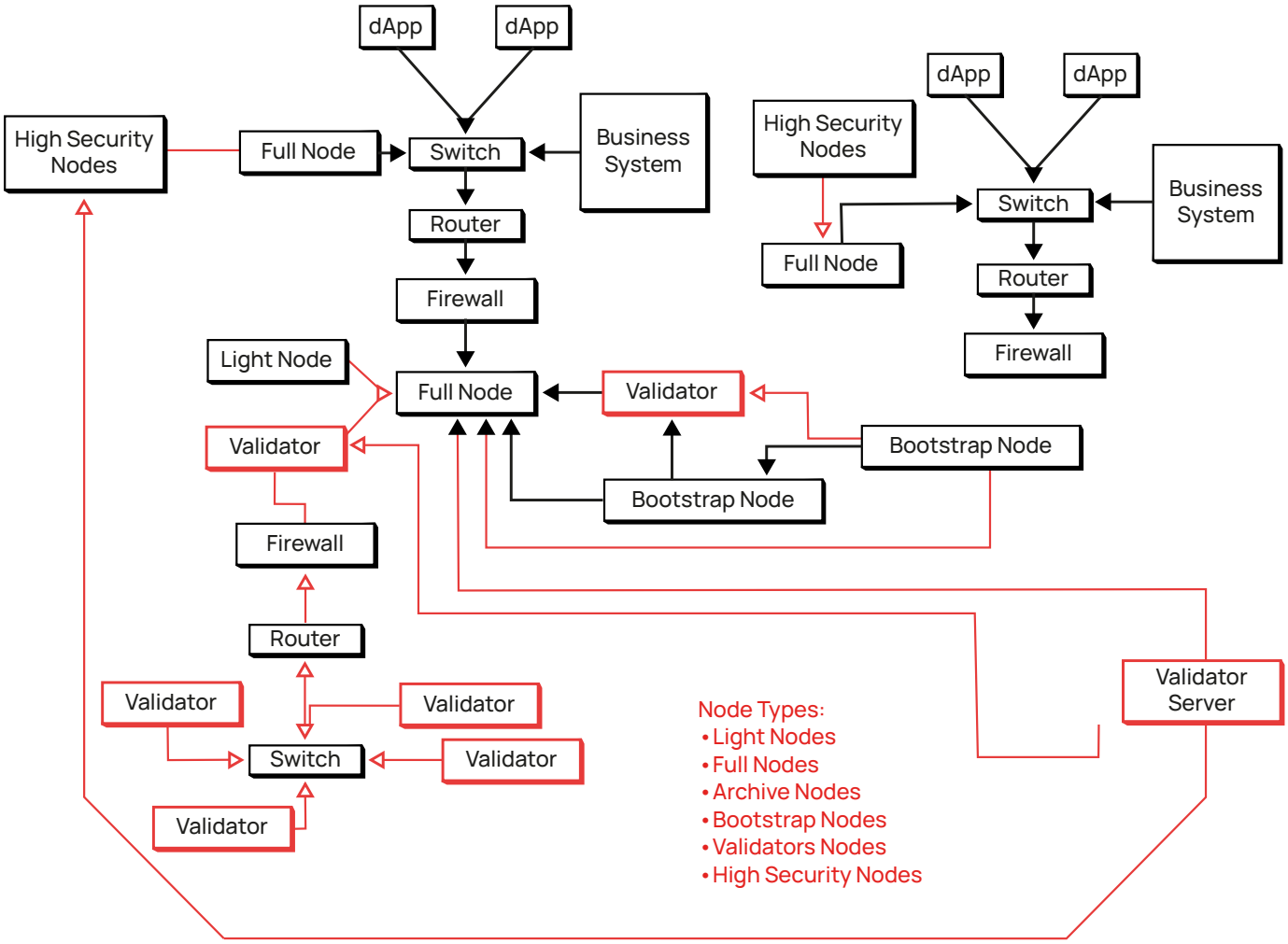
   a. Ecosystem
   This first group contains applications that provide common functions for the majority of the higher-level Blockchain applications. It comprises these categories.

   i. wallets.
   ii. exchanges
   iii. oracles
   iv. filesystems
   v. Identity management
   vi. secure timestamping

   b. Applications of the Blockchain Ecosystem:
   The following group of types of applications is one that operates at a higher level and focuses on specific features that are used by the user. This category comprises higher-level applications that inherit security aspects from particular categories in the underlying ecosystem groups. This category comprises areas like

   i. e-voting
   ii. notaries
   iii. identity management
   iv. auctions
   v. escrows etc

Naoris Protocol is focused on filling in the gaps at various levels of the blockchain. It provides a common system that is systematically implemented with a use case in mind and continuously improves its understanding of its use case baseline and is therefore a higher probability innovation bed because of its distributed security use case, ahead of most recent developments in the generic use of blockchains. It is a model that can be used by companies or users to tackle CyberSecurity risks; it is a system that enhances the muti-layer blockchain use ethos.



Overview of a sample network context under the Naoris Protocol

6.2.2. Risk Assessment Component Model on Topography

Security models for risk assessment

1. **Owners**
   Blockchain users are the owners. They can run any type of node and operate in both the applications or consensus layers. Owners of $CYBER tokens are able to use and offer applications and services that are based upon blockchain technology to others. Owners can also add consensus nodes that earn crypto-tokens when they run, offering a resilience service to the consensus protocol.

2. **Assets**
   Assets can be found at the application layer and can include:

   a. Monetary value, in other words. crypto-tokens and other tokens
   b. The availability of service-layer applications and functionalities built on top of blockchains such as for example notaries, escrows or data provenance, auctions, etc
   c. The authenticity proofs of/for users, privacy of users and privacy of information

3. **Threat Agents**
   They may be available at all levels and involve malicious users who are trying to take over

assets, disable functionalities or disrupt services. Threat agents may also include entities that are inadvertent entities such as smart contract developers who accidentally create bugs or designers of blockchain applications that make mistakes or ignore problems.

4. **Threats**
   Threats can enable the attack of assets on all levels. They're caused by flaws on the internet, the smart contract and applications that suffer from consensus protocol deviations, and breaches in consensus Protocol assumptions.

5. **Measures**
   These measures guard owners from threats by reducing the possibility of assets becoming lost, subverted or compromised. These solutions comprise:

   a. security/privacy/safety solutions
   b. incentive schemes,
   c. reputation techniques, etc.

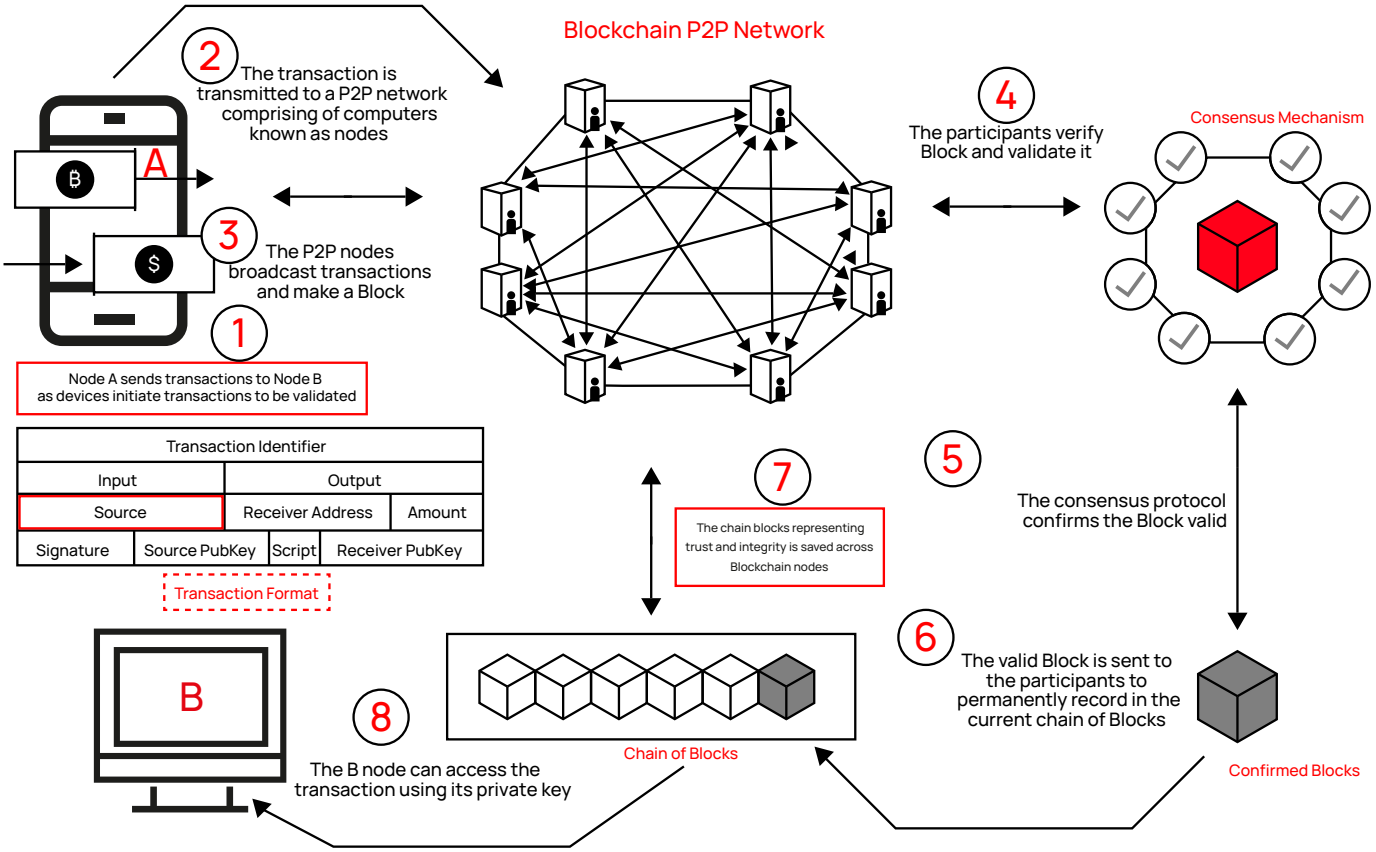
6. **Risks**
   The application layer is where risks are observed. These are generally brought about by threats and threat agents. It includes:

   a. Loss in monetary assets
   b. Privacy breaches
   c. Loss of reputation
   d. Service failures

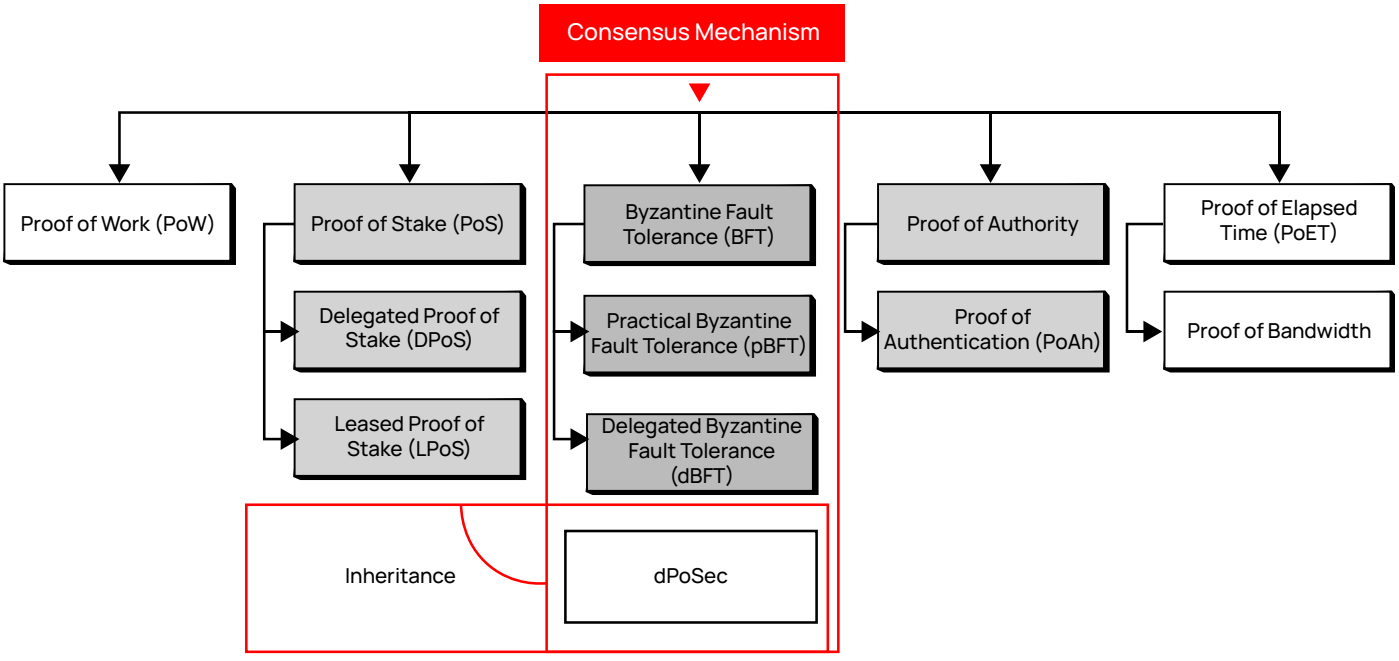
6.2.3 Threats vs Layers - Topography Risks

	The following are the threats to this layer:	Naoris Protocol suggests the employment of:
Application Layer	- False data feeds, - Censorship - Front running attacks, - Disruption of the availability of central components - Privacy and confidentiality - TEE (Trusted Execution Environment) manufacturer that is not behaving properly or is abusing its access/permissions - Faults in TEE	- Hyperstructure based integrity model for privacy preserving-constructs - Distributed multi-factor authentication enforcement - Distributed Integrity management with wallets - Redundancy /decentralization - Distributed reputation systems, etc.
Replicated State Layer	- Intentional/unintentional/semantic bugs in smart contracts - Risky cryptography constructs such as for example non-interactive zero knowledge proofs, blinding signatures, ring signatures, homomorphic encryption and many others that allow for risks to be present such as compromising the security of data of users and of identities.	- Safe language verification - Smart-contract vulnerability auto-verification - Analysis at static/dynamic levels - Formal verification -Distributed Audits - Distributed Definition and enforcement of best practices and design patterns - Distributed Zero-knowledge proofs support, etc.
Consensus Layer	- Malicious nodes could alter the outcomes of consensus protocols. - Malicious nodes may be able to take over the execution	- Incentivized scheme - Strong consistency across nodes, across Verge Clusters - Decentralized Mesh of nodes across shard-like structures known as Verge Clusters - Fast finality
Network Layer	- Man-in-the-middle (MITM) attacks - Network partitioning - De-anonymization - Constant availability	- Quality of Availability enforcement for nodes - Distributed naming validation using DIVA an SPOE - Protection of routing - Protection of anonymity through ZK-Proofs - Managed encryption standards for Data protection

6.3. Understanding the dPoSec Consensus Mechanism



dPoSec Consensus Workflow Overview [8]



[8] https://www.sciencedirect.com/science/article/pii/S2096720921000014#fig2

The dPoSec Consensus utilizes an innovative "rationality clause" mechanism to improve both security as well as decentralization efficiency within its consensus design. dPoSec is proposed to be an extension of the Byzantine Fault Tolerance protocol (BFT) that operates in asynchronous mode, where there is no upper bound on when the response to the request will be received. Its goal is to solve the many problems associated with already available Byzantine Fault Tolerance solutions. This new enhanced algorithm being "one solution to many problems", offers to solve the security and efficiency problems that lie with partially synchronous networks.

6.3.1. What is Byzantine Fault Tolerance?

Byzantine Fault Tolerance (BFT) is the feature of a distributed network to reach consensus (agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information. The objective of a BFT mechanism is to safeguard against the system failures by employing collective decision making (for both correct and faulty nodes) which aims to reduce the influence of the faulty nodes. BFT is derived from the well known Byzantine Generals' Problem.

6.4. The Byzantine Generals' Problem

The problem was explained aptly in a paper by LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE at Microsoft Research in 1982:

1. Imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general.

2. The generals can communicate with one another only by messenger.

3. After observing the enemy, they must decide upon a common plan of action.

4. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching an agreement.

5. The generals must decide on when to attack the city, but they need a strong majority of their army to attack at the same time.

6. The generals must have an algorithm to guarantee that all loyal generals decide upon the same plan of action, and a small number of traitors cannot cause the loyal generals to adopt a bad plan.

7. The loyal generals will all do what the algorithm says they should, but the traitors may do anything they wish.

8. The algorithm must guarantee the condition regardless of what the traitors do. The loyal generals should not only reach an agreement, but should agree upon a reasonable plan.

Byzantine fault tolerance can be achieved if correctly working nodes in the network reach an agreement on their values. There can be a **default vote** value given to missing messages i.e. *we can assume that the message from a particular node is 'faulty' if the message is not received within a certain time limit*. Furthermore, we can also assign a default response if the majority of nodes respond with a correct value.

Leslie Lamport proved that if we have **3m+1** correctly working processors, a consensus (agreement on same state) can be reached if **at most m processors are faulty** which means that strictly more than two-thirds of the total number of processors should be honest.

6.5. Types of Byzantine Failures

As stated under the "Impossibility of Distributed Consensus with One Faulty Process" - the problem of reaching agreement among remote processes is one of the most fundamental problems in distributed computing. A well-known form of the

problem is the "transaction commit problem," which arises in distributed database systems. The problem is for all the data manager processes that have participated in the processing of a particular transaction to agree on whether to install the transaction's results in the database or to discard them. The latter action might be necessary, for example, if some data managers were, for any reason, unable to carry out the required transaction processing. Whatever decision is made, all data managers must make the same decision in order to preserve the consistency of the database.

Reaching the type of agreement needed for the "commit" problem is straightforward if the participating processes and the network are completely reliable. However, real systems are subject to a number of possible faults, such as

- process crash
- network partitioning, and
- lost, distorted, or duplicated messages

One therefore wants an agreement protocol that is as reliable as possible in the presence of such faults. According to the protocol, consensus is reached on a certain task message and is executed consistently. There are many types of errors in this process, but they can basically be divided into following categories.

- Node crash, network failure, packet loss, etc within Non-Malicious Nodes

- Node crash, network failure, packet loss, etc due to Malicious Nodes. For example,

    - Failure to return a result - the validator can delay or reject messages in the network,

    - Respond with an incorrect result - the proposer can propose invalid blocks, or
    - Respond with a deliberately misleading result - the node can send different messages to different peers.
      In the worst case, malicious nodes may cooperate with each other.

6.6. BFT As A Solution From 10000 Feet

The applicability and efficiency of consensus protocols are governed by three key properties (Baliga, 2017).

- Security: A consensus protocol is said to be safe if all nodes produce the same output and the output produced by the nodes is valid according to the rules of the protocol.

- Liveness: A consensus protocol is said to be live if all non-faulty nodes participating in consensus eventually produce a value.

- Fault tolerance: A consensus protocol is said to be fault tolerant if it can recover from the failure of nodes participating in consensus.

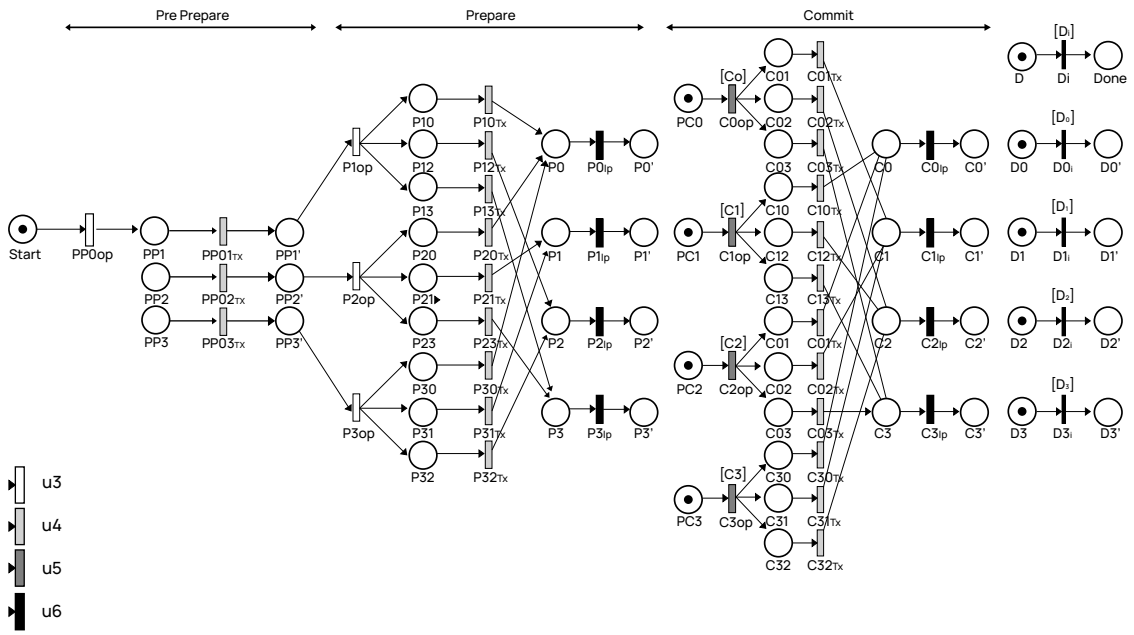
In simpler terms, liveness guarantees 'something good eventually happens' and safety guarantees 'something bad does not happen'. Thus safety and liveness are inseparable properties of fault-tolerant protocols.

According to Fischer et al. (1982), in a deterministic asynchronous consensus system, it is only possible to have at most two properties among safety, liveness, and fault-tolerance. Distributed consensus protocols compromise on one of the properties to drive blockchain-based systems for achieving desired goals.

Considering the errors, a system must always maintain:

1. Security
   1. Nodes must not produce incorrect results even in the case of errors, and must respond as per the rules of the protocol.

2. Liveness
   1. All non-faulty nodes must continuously generate submissions to produce a value



BFT based pBFT Phases Overview

Byzantine Fault Tolerance Protocol (BFT) is a protocol that guarantees the security of distributed systems regardless if malicious nodes exist within the system. Leslie Lamport proved that when we have 3m+1 correctly working processors, a consensus (agreement on same state) can be reached if at most “m” processors are faulty which means strictly more than two-thirds of the total number of processors must always be honest. When you look at the network the acceptance to commit it is situated upon 2f+1 votes, where “f” is the number of malicious processors and the total number of processors plus leader makes it “3f+1” in the network.

Generation 3	Hyperstructure, Multi-Chain, Cybersecurity, Scalability, AI
Generation 2	Sidechain, Data Exchange, Bridges, Onchain and Offcain Solutions
Generation 1	Consensus, Smart Contract, Trustless Network
Generation 0	Nework, Transportation, Storage, Discoveries

6.6.1. Consensus for a HyperStructure of Cyber-trust

dPoSec is a uniquely Cyber-Risk-Aware consensus mechanism that is used within the Naoris HyperStructure, including an add-on list of advantages. To meet consensus as a Generation 3 solution, it focuses towards enhancing the potential of the blockchain to be more efficient and to operate under fully decentralised CyberSecurity rules, that can also be optimised as a CyberSecurity solution for other systems and infrastructures. It can scale by delegating Cyber-Risk related responsibilities and telemetry to itself, working with, and in parallel with the operational processes available within its deployed Web2 or Web3 environments.

This part of the paper presents why dPoSec can be a Generation 3 implementation. dPoSec at its core focuses on its major use case, under the HyperStructure`s ethos. With the highest

resistance possible in mind, it is unstoppable and will be in operation for as long as the underlying blockchain is in existence and there are participants. There is a minimally extractive principle in order to maintain operations and rewards with maximum benefits - the larger the number of participants and Verge Clusters the higher its resilience and speed. There are also built-in incentives for those who participate in it as well.

It is universally available and resistant to censorship, in other words, no participant can be blocked from creating or participating in a public VergeCluster. It is user-agnostic, platform agnostic and use case agnostic, and finally, it adds to a positive summation as it creates a win-win environment for the participants in terms of the benefits they extract and provide, and from the same distributed infrastructure of infrastructures.

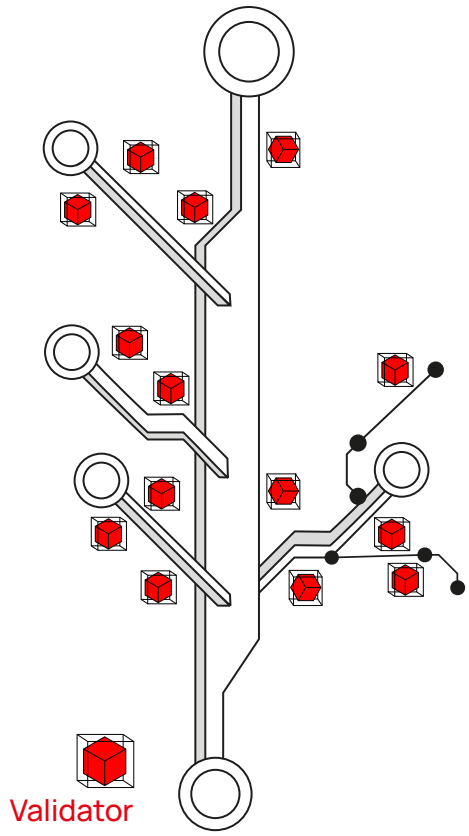
In the face of Byzantine adversaries, such an approach is highly resilient, this concurrent nature allows the attainment of speedy throughput and is highly scalable while leadership-free. Internal Verge Cluster rules and standards can be modified through voting.

6.6.2. Consensus Overview

6.6.2.1 Distributed Proof of Security (dPoSec)

dPoSec is targeted to communicate within 'secured mode', to reduce the overall complexity of the blockchain network during communication and provide improved efficiency for block production. Scaling itself towards a Phase-3 solution it additionally offers:

- Unstoppable network
- Permissionless network
- Valuable network
- Credibly neutral
- CyberSecurity based upon trusted nodes where one node validate other nodes for secured communication and processing
- AI based insights based upon privacy-by-design architecture
- Enhanced and efficient data block submission along with scalability and minimally extractive cost or possibilities to run with a zero-fee cost
- Extended to authenticate bad smart contract design and vulnerabilities prior to switching live. Offering assistance to repair vulnerable smart contract by 95.5% with correction ratio of about 93.32%
- Extended support of WASM for smart contract



Overview of a sample network context under the Naoris Protocol

Validators are nodes jointly selected by all $CYBER holders to maintain and develop the dPoSec network. The majority of nodes with the most votes will become alternative nodes, from which a core of validators will be randomly selected to participate in the management of the entire dPoSec network. The responsibilities of a validator are:

1. Maintaining node and the network operations
2. Produce and validate blocks
3. Proposal voting and decision-making

Minimum staking of a set amount of $CYBER tokens are required for a staking account, locked or unlocked. If the actual stake is less than the minimum staking amount due to penalties or any other reason the node will disappear from the listing of possible node candidates. There are also checks that entail the enforcement of the availability of recommended hardware levels, software and infrastructure requirements for the node.

6.6.2.2. Types of Validators

- **Potential Validators**
  This validator group creates a pool of potential candidates, i.e., the ones who will receive the most votes are potential validators. They participate in the validator selection process and are eligible to receive additional distribution bonuses.

- **Validator**
  The system randomly selects a number of validators from the potential validator groups and allows them to participate in consensus rounds. Prior to a block's finalization, they must be approved by a group of chosen validators.

- **High Security Nodes**
  The node holds a very low capacity of blockchain data management, unlike full nodes, and is responsible only to verify the blockchain. They are part of the Verge Cluster deployment and perform periodic executions to verify the existence of invalid or fraudulent blocks on the basis of the block header received from full-nodes. They are eligible to receive additional distribution bonuses.

6.6.2.3. dPoSec Protection Layer

Denial of Service for a Leader

dPoSec is a protocol that has been extended from the baseline of BFT consensus. BFT protocols don't assume or detect the presence of any risky or malicious devices, whose aim is to derail the protocol. This vulnerability, being exploited, can result in a situation where a leader in the round could be affected because its leadership is publicly known prior to the start of the round, causing a DoS on the Leader. dPoSec aims to protect against attacks like this using Verifiable Random Functions (VRF) and instantly publishes a block candidate following the publishing of the information.

Selfish Mining

An adversary tries to create a secret chain that becomes visible to the public only when the honest chain is "catching up with" the secret one. The longest-chain rule causes honest block producers to be included on the chain that is associated with the attackers and invalidate the genuine chain, thus reducing the power of their consensus capability. dPoSec suggests an automatic protection scheme against all these attempts since the protocol's core is based on a motivation based scheme. It follows the fork-choice rule that uses pseudo-random partial assistance for POS instead of POW.

Feather Forking and Bribery Attacks

With feather-forking, adversaries attempt to influence block producers' behavior by inflicting threats to harm their earning capability or by

executing bribery attacks in which adversaries provide specific rewards to block producers directly to allow attacks such as double-spending. dPoSec does not support POW to avoid and prevent any such threats. In addition, dPoSec maintains a close eye on the network for attempted attacks, and provides the possibility of providing rewards to other participants who report any such behavior and, at the same time, punishing such chains immediately while mitigating side channel attacks with stake slashing.

Posterior Corruption

Posterior corruption, the attacker is required to take/steal private keys from a majority of possible "retired" consensus nodes and then run the consensus protocol, writing a new timeline of blockchain. The dPoSec incentive program, along with the evolving algorithm for cryptography, secure digital signatures with forward-looking technology and the ability to implement irreversible checkpoints after an arbitrary amount of blocks, renders the network secure from an attack of this kind.

dPosec is also able to protect against a variety of other blockchain attacks such as lie-in wait, block withholding, specific pool attacks, etc.

Transaction Integrity Protection

In most of the blockchain stack available, transactions containing plain-text data are digitally signed by private keys of users, enabling anybody to verify the validity of transactions with the corresponding public keys. However, such an approach provides only pseudonymous identities that can be traced to real IP addresses (and sometimes to identities) by a network-eavesdropping adversary, that can after some degree of effort have a really high probability of guessing the identity of the participant successfully, and moreover, it does not ensure the confidentiality of data.

Zero-Knowledge Proofs and Mitigation of "Front-Running" Related Issues

Zero-knowledge protocols enable the transfer of information and proofs throughout the peer-to-peer blockchain network in a manner that is completely private and reveals only what needs to be revealed when it comes to proof without providing any additional information about the sender or set context. For instance one party - the prover - proves to some other party - the verifier that they understand the value X, without conveying any additional information independent of the fact that they understand the value.

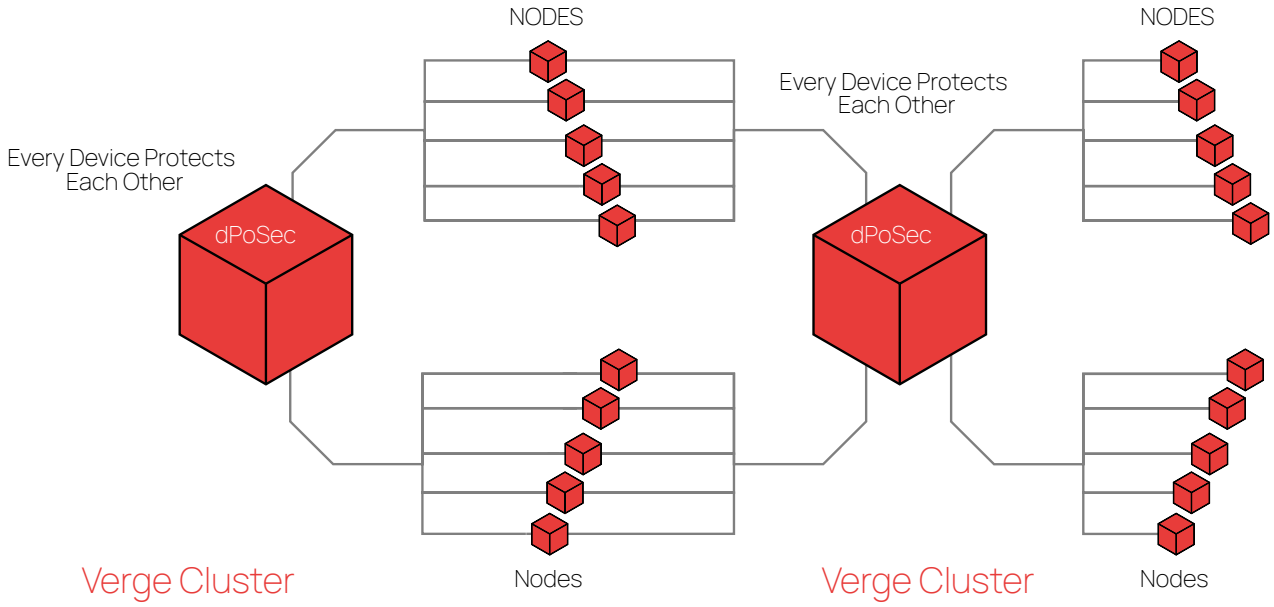
In normal blockchain transactions when an asset is transferred from one party in the network to another party, specifics of the transaction are known to all other parties within the network. In a transaction that is with zero-knowledge all the other participants only have the knowledge that a valid transaction occurred and nothing else about the sender or recipient assets, class of asset and other information. If proving a statement requires that the prover possess some secret information, then the verifier will not be able to prove the statement to anyone else without possessing the secret information. The statement being proved must include the assertion that the prover has such knowledge, but not the knowledge itself.

dPoSec uses decentralized privacy-preserving techniques based upon layered encryption along-with signature verification and zero-knowledge proofs. The Protocol is extended with trusted secure multiparty computations to preserve privacy and confidentiality.

6.6.2.4. dPoSec and Verge Clusters

First, a block that is derived from a Verge Clusters' potential validator, has been proven to be distributed to at least 51% of potential validators within the VergeCluster.

From these potential validators within the Verge Cluster, an undetermined set of potential validators are selected as chosen validators. The chosen validators then have the option of responding to the core block by raising a "rationality clause" or continue to operate as normal.



Distributed Consensus Overview within a Verge Cluster

If there are no rationality clauses raised by any chosen validator, then the block is deemed to be completed and the hash is stored in the blockchain.

The submitted block is later re-verified by High Secured Nodes and an extra validity check associated with the submission is performed, alongside the assurance that it was submitted from trusted validators only.

In an extreme case, if only one chosen validator is able to raise a threat risk then other validators in Verge Clusters initiate an entire consensus process that involves all potential validators for this Verge Cluster.

In an extreme case, if a chosen validator appears faulty or tries to participate along with other nodes to influence the whole network, the submission will not be attended to.
There is a distinct set of potential validators that are not part of the Verge Cluster, that are required to attain a complete Byzantine fault-tolerant consensus, that is 51% in order to complete the block.

This significantly improves security since the single chosen validator who is honest, or deemed to not be subverted or otherwise tampered with, is able to block an attack by any of the fraudulent potential validators.

As an added assurance layer in the context of risk mitigation, this can also be defined as a hyper-resilient layer of security, because all chosen validators are randomly selected, a potential threat actor would have to successfully compromise all nodes, as the chosen validator pool is not known before each consensus cycle, therefore complexity and obfuscation of potential validators is crucial and used as a de-facto resilience and defense mechanism. The fact is that only those who validate at every core cycle are aware of who the chosen validators are for that cycle, and will change again in the next cycle.

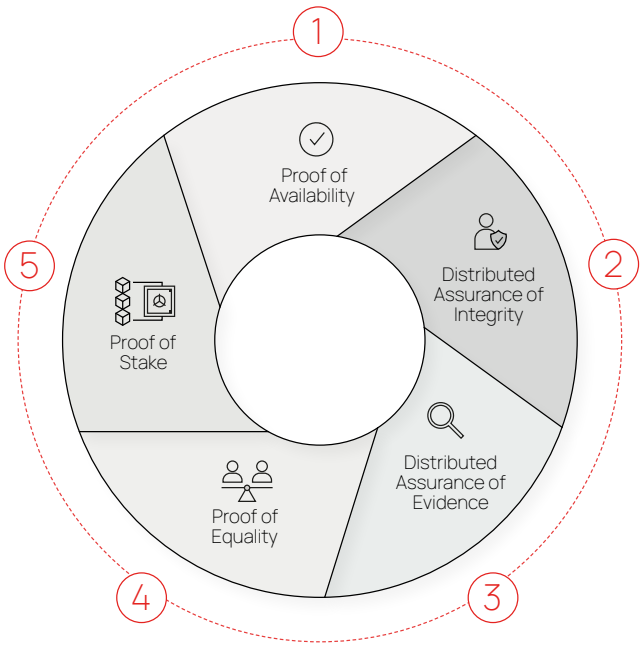
It's virtually impossible for malicious nodes to coordinate attacks between chosen validators and potential validators. In order for an attack to be successful with full assurance of outcome, all potential validators would be required to be malicious, since chosen validators are randomly chosen at each consensus cycle from a collection of subsets of potential validators.

This fault tolerance is high enough to allow blocks to complete quickly, since there isn't any rational strategy to deliberately issue a wrong block.

The traditional PoS as well as PoW consensus mechanisms require that you employ long chain rules in order to get to the point of finality.

This is because there is a chance that a block issued is fraudulent or in error. However, this is not the case with Naoris Protocol because of its incredibly high level of fault tolerance and baseline resistance to subversion or tampering.

This means that blocks are generated rapidly by every core of Verge Clusters simultaneously, while being checked by randomly selected validators from each potential validator pool of the Verge Cluster sphere. This produces an impressive speed



dPoSec Distributed Consensus Overview of its various parts

The Various Parts of dPoSec are as Follows:

- dPoSec includes "Proof of Availability" that helps to establish trust based upon the number of milliseconds/seconds/hours/days that the device is available to submit blocks and the quality of its connection and system stability.

- dPoSec includes "Distributed Assurance of Integrity" to ensure under consensus that integrity and trust in key processes are maintained, this also ensures that communications are happening from devices that are safe and secure. The devices remain under contentious monitoring and act as passive-active/server-client watchdogs to meet the defined standards of a specific VergeCluster.

- dPoSec includes "Distributed Assurance of Evidence" that proves trust during participation by exchanging additional information (known as detective evidence) during communication or validations.

- dPoSec also inherits features from “Proof of Stake” to manage rewards.
  To avoid such trust-related-threats, possibilities such as an uneven majority of the tokens being in the hands of only a few participants/validators, and the possible creation of an alternate blockchain history controlled by only a small number of private keys.

- dPoSec includes “Proof of Equality”, to distribute equal participation rights to earn rewards and spread the range of acquisition of potential validators across the Verge Cluster tree through Distributed Resilient Potential Validator Class (DRAPF).

6.7. Distributed Resilient Potential Validator Class (DRPVC)

Naoris implements what we call the Distributed Resilient Potential Validator Class, they are validator groups that exist in a continuous validation stream or groups of validation streams, without epochs.

This means that potential validators are able to move into and out of the validation stream or class at any point without epochs and with no resulting security risk.

Alongside the continuously changing sets of potential validators, Naoris has developed its own system for the aggregation of stakes in community pools.

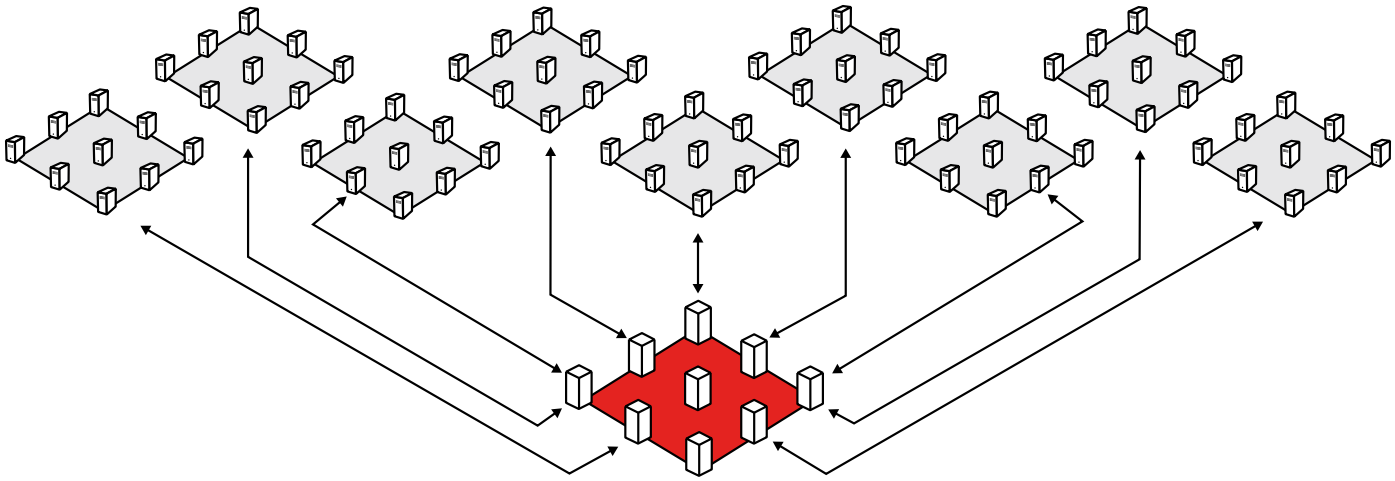
This combination of features is known as DRAPF. Naoris Protocol is the very first environment to introduce a system of community-based potential validators for a critical use case such as CyberSecurity.

They allow different entities to pool their efforts and $CYBER tokens for the purpose of becoming potential validators on their own for their own VergeCluster.

This method of simplifying Verge Cluster creation and distributing an ever-changing potential validator class, spread around various use cases like security validation level complexity, use case or geography for example, allows an even greater number of people to be potential validators which will undoubtedly result in a greater Distributed Resilience from a set of potential validators.

This increases decentralization which means there’s no dependence on a tiny group of potential validators - it also increases security, as potential validators have different rules/use-cases and can’t easily collaborate or be forced into collusion by a threat actor.

Verge Clusters

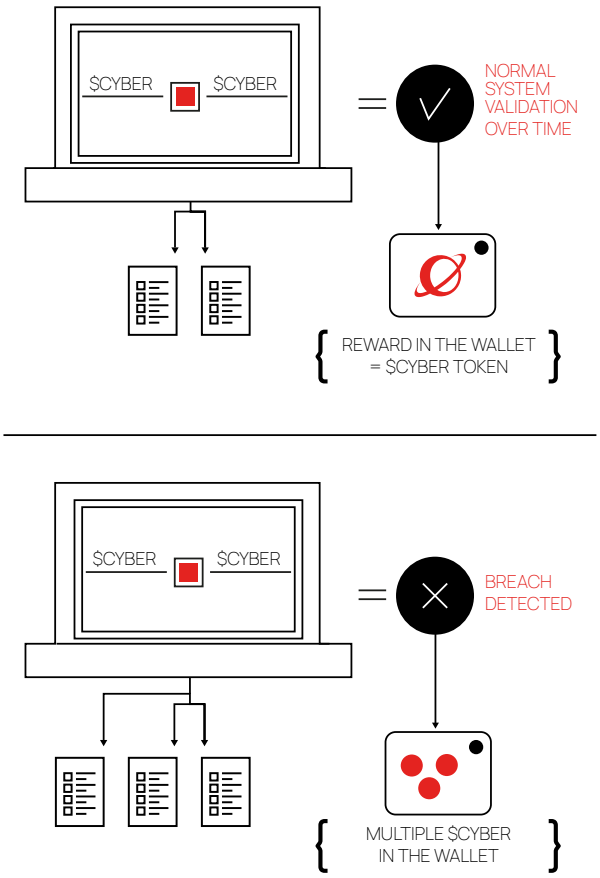


Naoris networking view with a plethora of connected verge clusters and their separate meshes

A class or group that has potential validator points is known as a potential validator class.

Potential validator classes are made up of various nodes from different validation streams and Verge Clusters. This stops untrue or fraudulent behaviour from becoming a pattern along with ensuring the baseline trust at the user level, OS-level and service level that would otherwise create a plethora of risks for the overarching trust network.

A distributed potential validator set (DRPVC) is the method by which Naoris can provide safer and speedier verification of transactions within its blockchain, at the highest criticality levels and most highly regulated and critical use cases.



$CYBER Network rewards overview upon dPoSec consensus

6.7.1. Powering a Tokenized Machine Economy for Distributed CyberSecurity with the $CYBER Token

With dPoSec we are working to create an alternative, which is more secure, efficient, transparent, inclusive, scalable and equitable for everyone.

dPoSec is based upon Validators and Potential Validators with extended pBFT + POS consensus that can support near-zero fees. dPoSec is EVM-compatible.

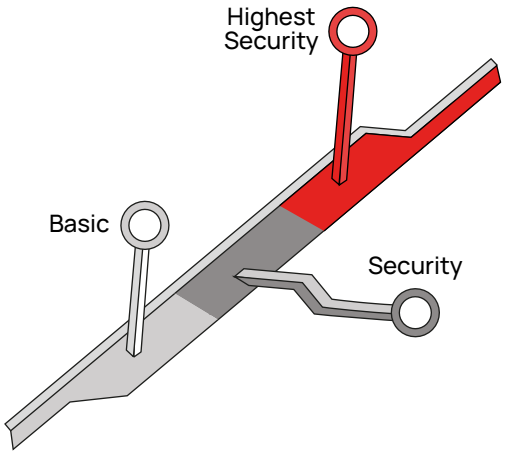
6.7.2. The Ecosystem

There are two key roles in the Naoris ecosystem:

- Users who subscribe to the platform's CyberSecurity services, and Validating nodes who validate work on the system.

The platform's advanced encryption techniques at its core-tier ensure the safe and secure processing and storage of critical, or sensitive metadata. The mechanics of the platform work the same way in each tier, but with additional security precautions.

The Naoris approach is very scalable, and capable of serving highly complex systems. That makes it a great fit for CyberSecurity-sensitive clients like enterprise, highly regulated or critical systems, governance structures, defense infrastructure or hybrid hosting services, on premise or cloud.



Levels of validation standards across the protocol

Users of the Naoris platform can include companies, networks, and individuals that endeavour to create and maintain their own Verge Cluster for their own use case and cyber-criticality level.

Nodes:

1. Full Node

2. Potential Validators
   Cyber token holders who want to participate in the production of the block, must commit to lock a certain number of tokens into the staking contract and become potential validators. Networks can have unlimited potential validators and are liable to gain additional bonus scheme benefits, must qualify to be among the most stable systems on the network to qualify. Ranking will be managed via an inbuilt trifecta Trust VS Availability VS Standardization ranking engine.

3. Validator
   Among the qualified nodes, the system randomly selects a subset as consensus round validators, their count is dependent on the overall network of network size and is dynamic, it is supported by an algorithmic random function. Validators on the network receive block rewards for the work they do to secure the network, which bootstraps engagement by giving them an intrinsically valuable stake in the platform and a vested interest in keeping it secure.

4. High Security Nodes
   High Security nodes check validity of blocks, and will generally share a portion of the reward for their work.

5. Light Nodes
   They are light nodes used to identify/validate block submission.

Staking

To become a qualified potential validator, high security node or validator you need to stake a predefined amount of $CYBER.

6.7.3. Consensus Rewards

After the successful commitment of a block, a protocol-defined amount of new tokens are going to be rewarded to all or any validators who signed the block in proportion for their voting shares. The transaction fees are rewarded to validators similarly as well.

6.7.4. Stake Slashing

For any misbehavior that is detected by the network, a specific quantity of tokens staked will be slashed. For instance, if an individual fails to finish his/her consensus procedure and initiates the leader change process the staked tokens will be reduced.

If validated users are found to have signed a fraudulent block, then each vote of their stakes under that specific Verge Cluster is slashed. This is a severe penalty put in place to discourage any fraudulent conduct and ensure that the network is as secure as possible.

Proof of misconduct could be two blocks signed by the same validator which conflict. Anyone can submit a transaction in order to prove that another validator has been misbehaving and if the proof is confirmed the slashed token will be awarded to provers.

6.7.5. Naoris Distributed AI Enabled Intelligence

“Swarm intelligence is the collective behavior of decentralized, self-organized systems, natural or artificial”.

It all goes back to nature and biology where organisms like ants, bees, birds, fish and many others form swarms, colonies, flocks, etc... to amplify their collective intelligence.

Across the world in various ecosystems we can observe that these organisms work together as a collective to solve problems and make decisions that surpass and are more efficient than individual organisms. The name given to this in science is Swarm Intelligence.

On the other hand, we humans don’t have the natural connections that other organisms have to ensure close and fast feedback-loops between them. These organisms have natural abilities to detect anomalies in their environment such as high speed vibrations (bees) or tremors in the water around them (fish). We humans can now utilize modern real-time and high speed networking technology to ensure close and fast feedback-loops between us and not only locally, we can do it globally too.

We at Naoris are working to develop Swarm AI technology that will allow the AI on each device to communicate in real-time with each other in whatever environment they are and wherever they are to assess new and existing threats. The integrated solution self-learns and trains itself for precise and effective decision making.

Swarm Advantages

1. Millions of AIs, one single emergent intelligence
2. Large quantity of AIs is essential
3. AIs interacting with each other locally
4. AIs follow simple rules
5. Decentralized approach
6. Extremely adaptive
7. Emergence of intelligent, collective, self-organized, global behavior
8. Randomness enables the continuous exploration of the alternatives
9. Efficient and fast resolution
10. Help with continuous monitoring and learning from “critical mass” to hold control over the risk.
11. Robust - Tasks are completed even if some AIs fail
12. Scalable - From a few to millions
13. Decentralized - There is no central control
14. Parallelism - AIs operations are innately parallel
15. Adaptation - The system continuously adjusts to stimuli (new or not)

7.0. Team

David Carvalho
Founder, CEO & Chief Scientist

Accomplished Global Chief Information Security Officer with 20+ years at technical and C-suite levels in regulated and critical areas of business and governance. Advisor for multi $Billion businesses and nation-state level projects in the critical areas of Cyber Espionage, Cyber War and Cyber Terrorism.

Monica Oravcova
Co-founder & Chief Operating Officer

Experienced leader with 15+ years in IT and Cybersecurity for Telco, Finance and Manufacturing, led operations and executive teams for FTSE 100 clients AT&T, IBM and Apple, managing budgets over $100M. Passionate evangelist and thought leader for women in Deep Tech.

Guy Davies
Chief Marketing Officer

Blockchain strategy & growth specialist, with 17+ years in commercial sales and business development for technology and innovation brands. 5+ years working in the Blockchain space with various startups, including the original Boson Protocol team leading Partnerships.

Sumit Chauhan
Interim Chief Technology Officer

Technology CTO, speaker, publications reviewer and writer in the blockchain space. Advisor with 19+ years building and delivering enterprise level solutions focused on global growth and digital transformation using Blockchain and AI for CyberSecurity, IoT and FinTech.

Saurabh Jain
Head of Technology R&D

Performance technologist with 18+ years experience in Software Development and Project Execution, 3+ years implementing Blockchain enabled Enterprise Solutions across Hyperledger, Fabric, Ethereum, Algorand, EOS, WAX, in areas of Scale Design, Resilience and Fault Tolerance, Performance, High Availability and User Experience.

Scott MacAndrew
Interim Chief of Finance

With 25+ Years in Global Finance Portfolio & Hedge Fund Manager, Trader, Market-Maker, Investor. Career Focus : banking, trading, F/X, capital markets, FinTech, crypto, tokenomics, blockchain. Designations: CIM, Series 65, FCSI.

Jim Tousif
Head of Investor Relations

Managed over $250m+ in his 20 year career and mentored 100+ in startups, larger companies and a serial entrepreneur with decades of success in finance. Holds MBA from Haroun Education Ventures and FINTECH certification from Cornell.

Tony Sarvestani
VP of Business Development U.S.

Financial and software industry professional and top producer in multiple financial firms and business development for software companies. Have worked with fortune 500 companies advocating and providing strategies for global growth and future initiatives.

João Ferreira Santos
Head of Compliance

João is an experienced Regulatory / AML / KYC / IP Advisor. He has previously worked in Banco BPI, BNP Paribas and various startups at Managing Director level in Hong Kong. Holds a Law degree from the Faculty of Law of Lisbon University and is a licensed Lawyer.

Kwadjo Nyante
Lead Researcher & Content Manager

Expert in Advanced Cryptography and cryptanalysis, Identity Management and Distributed Ledger Tech. Security Leadership, Management and Strategy, CISSP professional. Worked on eIDAS, Blockchain self-sovereign identity, privacy by design with Homomorphic encryption and Crypto-Agility.

Vijayant Verma
Head of Data Science and Open Source Development
Technologist with 18+ years experience in BI, Blockchain, AI and ETL Development for business applications. Expertise in deployment of custom open source tools to fit business requirements. Fluent in Golang, Python, Nodejs, Java, and Spring.

Constantinos Antoniou
Social Media Analyst

Constantinos is an experienced Crypto Analyst and Marketeer. He previously worked as Head of Community at Panther Protocol and as Head of Research at D-Core.net managing a team of researchers and the development of the platform.

Gaurri Agarwal
Blockchain Developer

Experienced developer for dApps on Ethereum, Solana, Algorand, Hyperledger and working with consensus protocols like Proof-of-Work, Proof-of-Stake and Proof-of-Authority.

Puneet Nayal
Blockchain Developer

Expertise in Ethereum, Hyperledger, WAX, Solana, Tokens, DeFi Applications and Cryptocurrencies, with experience in both permissioned and permissionless blockchains

8.0. Advisors

Knut Grandhagen
Head of Communications, Norwegian Armed Forces Cyber Defense

Brendan Holt Dunn
CEO of Holdun Family Office

Elena Gaudette
Chief of Staff at Cisco Cloud Security

Nuno Almeida, PhD
University Professor at Instituto Superior Técnico

Miguel Oliveira, PhD
University Lecturer and Director of Software Development at University of Aveiro

Dr. Magda Lilia Chelly, PhD
Award-winning global cybersecurity leader and Top 20 most influential cybersecurity person 2017 & 2021 by ISFEC Global

Jane Frankland
Top 25 Women in CyberSecurity, UNESCO Trailblazing Woman

Jeehyun Chang
Blockchain Entrepreneur

Richard Baylie
CIO at OCS Group

Dennis Lee
Founder of Dexlab

Svein-Erik Nilsen
Cyber and Decentralization Ambassador

9.0. Acknowledgements

This White Paper is based on concurrent and recursive research in the areas of CyberSecurity and blockchain around the capability and promise for a completely novel Web3-based technique, employing HyperStructure principles to solve key hard problems within our global digital systems.

Taking place over the last seven years, with conclusions and methods put into practice over the last two years, we are immensely grateful to our friends and colleagues for encouraging us to start, persevere, and finally publish this work.

From the UK, we thank Guy Davies from the Brixton Pound for his input with this whitepaper, Jane Frankland from 'IN Security Movement', Richard Baylie and Ali Jooyand from OCS Group leadership and security teams, Ninva Ponsonby for her help and support, and many others for the enterprise level backing, academic level thought leadership support and ongoing honest friendships.

From India, we are grateful to our friends and team members who never stopped challenging us to do more, aim higher and when faced with tough tasks, showed courage and the amazing capability to think laterally, solving the most complicated issues and use cases that an unusual innovation project like ours presents. We would like to extend our best regards and respect to their work and dedication in helping us develop our ideas further.

In the US and Brazil, we thank colleagues Jim Tousif for his unyielding perseverance and friendship, Elena Gaudette from Cisco Cloud Security for her visionary support since the very beginning, Bruno Ahualli for the deep strategic input and Michel Turtchin for adding his artistic skills to the project.

From Portugal we would like to extend our gratitude to Monika Oravcova who has been a fundamental pillar to the project since its idea phase, leading our path through the world`s best accelerators and events; Nuno Almeida from the Instituto Superior Técnico University for his partnership and principle-centered guiding force, and to João Ferreira Santos for his energetic legal and compliance guidance.

A special word of gratitude is due to Scott MacAndrew from Holt / Cypher and Brendan Holt Dunn from the Holdun Family Office, for showing confidence in our work at key junctures and for their steadfast support from the outset. To Brian MacMahon from the Expert Dojo Accelerator for his advice and support, to Oliver Schwabe we would like to extend our thanks for our partnership on European projects and Smart Cities Initiatives in the area of Decentralized CyberSecurity Meshes and Protocols. We thank you all for working with us through the long process of evolving the protocol concept, and for your friendship and help.

A special thanks to the dozens of mentors from key industry spaces across the world-class accelerators we were finalists in, from the US, Canada, Chile, Austria, Portugal, and South Korea.

From Norway our thanks go to Svein Erik for accompanying and supporting the project since the very beginning as a colleague and friend, Knut Grandhagen from the Norwegian Armed Forces Cyber Defense for his long standing support and belief in our project, and Firoz Shroff for his unique insights, lateral thinking and mentorship in business.

We would like to dedicate the successful culmination of the first milestone of this momentous effort to the memory of our friend and mentor, Kjell Grandhagen, the former Chairman of NATO/OTAN Intelligence Committee. Kjell's approachability, inspiration, foresight and vision around the fundamental need for the decentralization of CyberSecurity principles within the highest areas of criticality in society and beyond, helped inspire the whole project. His unwavering stance on key principles for society and geopolitical initiatives gave us the confidence to shape the path forward since the very first test phase, aligning his support in both the media and other key opinion pieces.

Finally, we would like to acknowledge with gratitude, the support and love of our
Families - they have all kept us going, and this project would not have been possible without them.

10.0. Disclaimer

THIS PAPER HAS BEEN DRAFTED AS A NON-BINDING THOUGHT PIECE REGARDING A POTENTIAL FUTURE PROJECT INVOLVING $CYBER TOKENS. PLEASE NOTE THAT $CYBER TOKENS HAVE YET TO BE DEVELOPED, AND THEIR FUNCTIONALITY MAY DIFFER, AND BE COMPLETELY DIFFERENT FROM, THAT SET OUT IN THIS PAPER. ANY POTENTIAL ACQUISITION OF $CYBER TOKENS WILL BE ON THE TERMS OF A SEPARATE AGREEMENT, AND THEY ARE PROVIDED SOLELY ON THE TERMS OF THAT AGREEMENT. NOTHING IN THIS WHITEPAPER SHOULD BE READ AS CREATING ANY OBLIGATION OR EXPECTATION, EXPRESS OR IMPLIED, AS REGARDING HOW $CYBER TOKENS SHOULD OPERATE OR FUNCTION. PLEASE NOTE THAT CAPITAL IS AT RISK IF YOU MAKE ANY ACQUISITION OF $CYBER TOKENS. IF ANY PERSON IN RECEIPT OF THIS PAPER IS IN ANY DOUBT ABOUT WHETHER OR NOT AN ACQUISITION OF $CYBER TOKENS IS COMPATIBLE WITH THEIR INDIVIDUAL CIRCUMSTANCES OR NEEDS THEY SHOULD SEEK PROFESSIONAL ADVICE PRIOR TO MAKING AN ACQUISITION

NAORIS PROTOCOL

WhitePaper

Cybersecurity Mesh Hyperstructure for the Digital World

Version: 1.02.02