Decentralized Ledger Infrastructure
It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change.

~ Charles Darwin
## Contents

1. **Introduction** .................................................................................................................................................. 4

2. **Glossary** ......................................................................................................................................................... 5

3. **Introduction** .................................................................................................................................................. 7

4. **Challenges & Opportunities** .......................................................................................................................... 10
   - 4.1 Mobile Network Operators .......................................................................................................................... 10
   - 4.2 Internet of Things .......................................................................................................................................... 11
   - 4.3 Distributed Ledger Technology ..................................................................................................................... 13

5. **XENIRO Vision** ............................................................................................................................................... 17
   - 5.1 The xGRID – A New Network Paradigm ....................................................................................................... 17
   - 5.2 Applicable DLT Use Cases .......................................................................................................................... 23

6. **XENIRO Solution** .......................................................................................................................................... 29
   - 6.1 XENIRO Automation Platform (XAP): Multi-Access Edge Computing (MEC) ............................................. 29
   - 6.2 XENIRO SnapScale Hybrid DLT .................................................................................................................... 36
   - 6.2 XENIRO ORDOS ASIC ............................................................................................................................... 44

7. **Empowering the Ecosystem** ........................................................................................................................... 53
   - 7.1 Ecosystem Partners ........................................................................................................................................ 54
   - 7.2 XENIRO Economic Model ............................................................................................................................ 55

8. **Summary** ......................................................................................................................................................... 58

9. **Acknowledgment** ........................................................................................................................................... 61
Blockchain is a type of Distributed Ledger Technology (DLT), also known in the world as the “Trust Protocol,” that records transactions across a distributed global network of nodes. In this paper, XENIRO aims to address the exponential growth of the IoT industry evolving towards an Intelligent Machine Economy, where sensors are now connecting virtually every industry with built-in intelligence, across billions of devices. Increase in connected IoT devices is also attributed to Mobile Network Operators (MNOs) supporting technologies such as the upcoming 5G NR (5th Generation New Radio), Multi-Access Edge Computing (MEC) and Network Function Virtualization (NFV). This underlying infrastructure is critical in delivering connectivity at ultra-low latency, high bandwidth, high availability and performance at scale, serving the fourth industrial revolution.

We will exhibit the value of DLT architecture empowering business model innovation. Enabling billions of devices or machines themselves to conduct transactions autonomously across the distributed ledger through a tokenized protocol. Leveraging MNOs complementary agile and resilient infrastructure, in creating a new network, through MEC’s (distributed architecture) to achieve both security and scalability. This solution is the first of its kind. At XENIRO, we believe that a disciplined Decentralized Ledger Infrastructure will transform and accelerate the industries of tomorrow.
# Glossary

## XENIRO ACRONYMS

- **xGRID**: XENIRO’s definition of a new network centered around Multi-Access Edge Computing
- **DSPE**: DISTRIBUTED LEDGER SMART POLICY ENGINE
- **ORDOS**: XENIRO ASIC (Application Specific Integrated Chip)
- **SNAPSCALE**: XENIRO Hybrid DLT Blockchain Protocol
- **XVM**: XENIRO VIRTUAL MACHINE (Smart Contracts Code Execution)
- **XAP**: XENIRO AUTOMATION PLATFORM (xGRID Operating System)
- **XAD**: XENIRO ACCELERATION DEVICE (Embedded Hardware Device with ORDOS onboard)

### Glossary

- **3GPP** (3rd Generation Partnership Project)
- **5G** (5th Generation Network)
- **5G NR** (5th Generation New Radio)
- **Application Program Interface** (API)
- **Augmented Reality** (AR)
- **Business-2-Business** (B2B)
- **Business-2-Consumer** (B2C)
- **Business Support System** (BSS)
- **Byzantine Fault Tolerance** (BFT)
- **Capital Expenditure** (CAPEX)
- **Cloud-Ran** (C-RAN)
- **Central Processing Unit** (CPU)
- **Distributed Denial-of-Service** (DDoS)
- **Directed Acyclic Graph** (DAG)
Decentralized Applications (DApps)
Distributed Ledger Technology (DLT)
Delegated Proof of Stake (DPoS)
Direct Memory Access (DMA)
Electronic Vehicle (EV)
European Telecommunication Standards Institute (ETSI)
General Purpose Register (GPR)
GSM Association (GSMA)
Industrial Internet of Things (IIoT)
Internet of Things (IoT)
InterPlanetary File System (IPFS)
Machine-2-Machine (M2M)
Mobile Network Operator (MNO)
Multi-Access Edge Computing (MEC)
Network Function Virtualization (NFV)
Network Function Virtualization Infrastructure (NFVi)
Network Slicing (NS)
Operating Expenditure (OPEX)
Operating Support System (OSS)
Over The Top (OTT)
Platform As A Service (PaaS)
Proof of Work (PoW)
Quality of Experience (QoE)
Quality of Service (QoS)
Quantum Key Distribution (QKD)
Service Level Agreement (SLA)
Software Defined Networking (SDN)
Software Development Kit (SDK)
Time To Market (TTM)
Transaction per Second (TPS)
Virtual Reality (VR)
Zero Knowledge Proof (ZKP)
Zero Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs)
Digital transformation is defined as the integration of emerging digital technology, in all areas of the business and enables an organization to better compete in an economic landscape, that is continually changing as technology evolves. In practice, end to end customer experience optimization, operational flexibility, and innovation are key drivers and goals of digital transformation. Along with the development of new revenue sources and information-powered ecosystems of value, they lead to business model transformations. Successful organizations need to adapt to meet changing market expectations or face extinction. Organizations have to transform at a much faster pace today as a result of an abundance of technologies shaping modern customer expectations. In the following paper, we will examine the disruptive distributed ledger technology, combining the exponential growth of the IoT segment, leveraging the MNOs emerging 5G infrastructural technologies in securing a new level of open innovation through service differentiation.

The Statistics

**Mobile Economy**: According to the GSM Association (GSMA) and its “Mobile Economy 2018” report, mobile technologies and services generated 4.5% of global GDP in 2017, thus contributing to an equivalent of USD$3.6 Trillion of added economic value. The same report also predicted that the contribution will reach USD$4.6 trillion or 5% of GDP by 2022.

**Mobile Network Operators**: In June 2018, Forbes Global 2000 list claimed that the world’s top 54 Telecommunication companies totaled more than USD $3.4 trillion in combined assets and nearly USD $1.5 trillion in revenue the year before. The focus of their Capital expenditure (CAPEX) is building a resilient, secure and agile infrastructure that is well-governed in empowering the digital society.

**IoT Market**: IDC predicted in its Spending Guide Forecast, that the IoT market would experience a compound annual growth rate (CAGR) of 13.6% over the 2017-2022 period and reach USD $1.2 trillion in 2022. Business Insider estimated that there would be 24 billion connected things by 2020. Gartner predicted...
predicted 20 billion connected devices, outnumbering humans 4-1. Ericsson\textsuperscript{vi} forecasted around 29 billion devices by 2020 and Huawei\textsuperscript{vii} came up with a more aggressive exponential growth of 100 billion devices by 2025.

MNOs have entered the IoT market early, but because of the novelty of the paradigm, many aspects of the technology in this area are yet to be discovered. In effect, any network-connected objects are capable of financial and operational transactions, providing a tremendous amount of value within this ecosystem. IoT also opens up hosts of opportunities in multiple vertical markets.

**Mobile Network Operator capabilities**

**5G:** The 5\textsuperscript{th} Generation networks will begin to go mainstream in 2020 and promise to offer low latency, and high throughput (as fast as 20 Gbps + pending spectrum selection) but, most of all, unleash the potential of automation. 5G will bring unparalleled disruption to all segments of the markets with new business model innovation (Autonomous cars, Smart Cities, IoT, Immersive entertainment, communication & collaboration).

**5G Design Principles:** Network softwarization through the convergence of NFV (Network Function Virtualization), SDN (Software Defined Networking) and MEC (Multi-Access Edge Computing) are considered MNOs’ most strategic infrastructural assets in the 5G revolution. NFV is a virtualized back-end mobile core network that incorporates cloud and virtualization technologies in driving developments of differentiated network services. Enabling both management and orchestration of networking resources that support MNOs end-to-end infrastructure through Network Slicing (NS). This technology relies heavily on the support of SDN in both of the mobile fronthaul and backhaul. The fusion of NFV and SDN is an integrated 5G Transport Network that is a flexible, reconfigurable, with a software-defined transport architecture accommodating the demands of the 5G infrastructure.

**The Power of MEC:** Both 5G and MEC are considered disrupting technologies on their own. But combined, they become a mighty force in the computing world. 5G networking capabilities will increase the number of connected devices on a network. Spurring the need for a MEC architecture that is scalable and openly programmable at the edge. Together with MEC, they are capable of pushing the mobile network frontier all the way to the Radio Access Network (RAN). Through this combination, MEC essentially becomes distributed Micro data centers at the edge of the cellular network with unprecedented compute, storage and networking capabilities. Resulting in the benefits of reduced latency with Quality of Service (QoS), enhanced mobility and time to market. Opening up new values through innovative applications at the edge for the billions of IoT devices.
Figure 1 depicts a horizontal view of the MNOs infrastructure. With the introduction of 5G NR, an entirely new network is created with MEC servers at the edge. Opening new frontiers for MNOs to deploy XENIRO’s Distributed Ledger Technology (DLT) platforms, hosting decentralized applications (DApps) at the edge, in a containerized microservice architecture, proximity to the IoT devices. MEC possesses the networking & computing capabilities to reduce the latency for DApps and allow for the scaling of all IoT related network services that weren’t previously possible (MEC will enable MNOs to open up their Radio Access Network to authorized parties). They contribute to reducing the physical and virtual communication distance, by avoiding services being processed at the backend of the mobile core network. Creating an immensely powerful infrastructure.

**XENIRO’s Role**

XENIRO is an open MNO-focused Consortium DLT foundation, based on a hybrid consensus DLT protocol (SnapScale) that is articulated for performance and scale residing in the MEC environment. SnapScale DLT not only provides a standardized communications model to process interactions and transactions between IoT devices, but also allows for Security, Scalability with an optimal level of decentralization. This combination will incubate a new wave of IoT communities, thereby accelerating the on-boarding of decentralized applications (DApps) and unlocking extended monetization capabilities on a new network, with a new platform, in a new ecosystem.
4 Challenges & Opportunities

In the following section, we will begin to emphasize the opportunities associated within each of the industries in question, through assessing some of the challenges and opportunities.

4.1 Mobile Network Operators

MNOs provide the foundation for our rapidly changing digital economy. The networks they maintain ensure global connectivity, but they’re facing unprecedented pressure from stakeholders and customers to accelerate innovation, accommodate disruptive technologies, and differentiate their offerings. MNOs continuously face competitive threats from organizations commoditizing their traditional services (Also known as Over-The-Top OTT players) while the markets and their customers change at a relentless pace.

To seize the opportunities, MNOs must evolve at pace. To exercise their capabilities, they need to revisit and reposition their ecosystem through: (A) Type or customers (machines, connected things, new partnerships, new industries). (B) Service enablers (throughput, latency, security, groundbreaking applications, SLAs). (C) Leverage emerging technologies (5G, NFV, MEC, SDN). (D) building strong alliances and partnerships.

With emerging technologies, supporting end-to-end flexibility will be one of the defining features of the 5G networks built on programmable software’s. With this cloud native capabilities, the NFV infrastructure within the 5G framework will be able to automatically place the desired workload, to a designated computing architecture in the right facility at the correct location in efficiently delivering the services with an enhanced experience. In essence, it is all about scale, resilience, and speed. That is comparable to a distributed system, capable of scaling to tens of thousands of self-healing multi-tenant nodes.

MEC is a network architecture concept that enables integrated networking, computing and storage resources into one programmable and unified edge infrastructure.

MEC on the other hand, enables the node to run in an isolated environment from the rest of the network and creates access to local resources and data. MNOs can open their RAN edge to third parties to rapidly deploy innovative applications providing new ecosystems. MEC is complementary to the existing 5G implementation with deployment agility that can scale horizontally or vertically with the ability to cater for: Proximity, Real-Time, Location awareness, Robust performance, Conservation, and Resource availability.
4.2 Internet of Things

IoT is an ecosystem of ever-increasing complexity. It is highly regarded as the next wave of innovation that will humanize every object in our life through automation. However, this revolution is also generating an enormous volume of data for the telecommunications industry. Data gathered from in-store beacons, environmental sensors, and mobile devices have the potential to create value in new, unprecedented ways. MNOs must determine the best way to analyze and monetize this data. Current predictions suggest that by 2020,\textsuperscript{viii} smart sensors and other Internet of Things devices will generate at least 507.5 zettabytes of data. Cisco (GCI)\textsuperscript{x} predicted 847 zettabytes of data created by 2021. Trying to do all of the computational heavy lifting offsite ultimately becomes a limiting factor. Specific IoT applications will generate extremely high data rates that will be required to be examined in real time. It requires an architecture to process these instructions where MEC is mostly suited for staging requests, backed by computational resources at the edge.
IoT resides in an ecosystem that is currently built on a centralized architecture, also known as the server/client model. Devices are identified, authenticated and connected through cloud servers that provide computational and storage resources. One of the biggest hurdles of IoT is that it poses a wide range of new security risks and challenges. These threats can take the form of communication interception, physical tampering, within the platform and DDoS. The fact that many devices use simple processors and operating systems with weak design increase their vulnerability to advanced mass attacks. It is essential to frame and build a solution that involves both hardware and software with multi-levels of sophisticated cryptographic encryptions.

With the proliferation of IoT devices, this model has reached a bottleneck and is indeed no match for the growing ecosystem of tomorrow. Despite the difficulty in monetizing IoT devices, MNOs are expected to have strong market position in the future IoT verticals. Offering just connectivity does not leverage on MNOs’ all assets, and they need to reinvent themselves to become more than just a basic “connectivity providers” in the new IoT era. Eventually, their survival might depend on their ability to address this challenge.

While the industry continues to pour massive CAPEX spending into the centralized cloud data center model to scale up IoT solutions, this is ultimately the wrong strategy, where MNOs are recording low margins. Maintaining a centralized cloud infrastructure that includes large server farms and networking equipment’s requires extremely high CAPEX. In the new era of IoT, with evolving platforms, ecosystems and technologies, we need to eliminate this current status quo of processing everything through centralized data centers.

While IoT is an extension of the current Internet, the expansion of that “Value” can be derived from things making self-guiding decisions and interacting autonomously without any human intervention. Despite some of the promises and potentials, IoT still has to resolve rising concerns around: (1) unified standards, (2) privacy (3) security (4) device Monetization. To adequately address some of these dilemmas, we believe DLT may be the needed enabler and disrupter that the industry is longing for. This technology was previously prominent in the financial sector, but new, programmable types of DLT such as the SnapScale DLT, will become much more relevant in the MNOs industry. IoT of the future will not just be built on simple connectivity but deliver valued services through a distributed 5G MEC architecture operated via the SnapScale DLT. It will forever change the way we compete and disrupt through dramatically shifting the MNO dynamics in altering the competitive landscape.
4.3 Distributed Ledger Technology

The DLT is essentially a distributed database. Records in each block are verified through unique algorithms that assign a hash – a unique combination of letters and numbers - to each block. It is the hash that makes the information secure and encrypted. If any information is changed within the block, the algorithm will no longer produce the correct hash. Hashes are continuously checked for correctness, and the individual blocks are combined to form the blockchain. Due to the interlinking of these hashes, the information stored on the DLT cannot be tampered with, unless an entire chain is re-written before a new block is entered. This continuous verification process is performed by all or selected members of the community.

The industry is shifting towards DLT as the most capable technology to date in fulfilling the missing link to settle security, privacy, and reliability for the IoT. Perhaps a fit that the industry has been waiting upon. DLT on IoT is a powerful driver that allows the tracking of billions of connected devices, enables autonomous transactions and coordination. This decentralized architecture will eliminate a single point of failure, defining a more resilient, governed and secure infrastructure for devices to operate. Privacy and communication protocols can be protected through enhanced cryptographic encryptions on the DLT enabling a secure Peer-To-Peer (P2P) messaging exchange for initiating smart contract execution for IoT devices.

This decentralized, autonomous and trustless nature of the DLT becomes an ideal candidate as a foundation for IoT. The core driver of DLT is its capability to maintain a decentralized trusted ledger of all transactions occurring in the network through: (1) Creating Trusted “Things” (2) Providing a safe and secure environment for IoT devices to operate (3) Accelerating machine transactions with a decentralized edge infrastructural model (4) Allowing for business model innovation.
An interesting article from Heavy Reading, that identified several pillars whereby DLT has the potential to disrupt the MNO industry in various dimensions.

![Image](75x479 to 343x679)

As depicted in figure 2, increased security & new service opportunities are promising domains. They are highly suited to the IoT industry where enhanced security will be complementary to new service opportunities. Another exciting area identified is cost savings for settlement & clearing. This is an area for exploration where traditional OSS / BSS systems in operator network can be replaced with DLT for increased security and cost efficiencies.

**Scalability:** Ethereum and quite a few DLT players have so far proven that technology, decentralized systems, and global collaborative communities can somehow work to a certain extent. They have also revolutionized usability among certain elite developers’ community. However, they have fallen short of making the development of DLTs mainstream, that is easily adaptable and accessible to entrepreneurs, innovators and, corporations around the world. A new decentralized world awaits, but only if we can produce a new generation of DLT that solve some tough challenges in this domain. Due to the increased adoption of DLT in recent years, the number of users and transactions have skyrocketed, stretching the limits of early-generation DLT systems exposing the scalability plague.

**Storage:** Most applications that get built on a DLT will require storage solutions (user identities, financial information, etc.). However, storing information on a DLT database meant that the data is: (1) Stored by every full node in the network (2) Stored indefinitely as the DLT database is append-only and immutable.

The storage capacity and scalability of DLT are still under debate, but in the context of IoT applications, the inherent capacity and scalability limitations make these challenges much greater. In IoT, where devices can generate gigabytes (GBs) of data in real time, this limitation represents a barrier to its integration with DLT. DLTs are not designed to store large amounts of data like those produced in the IoT. Majority of IoT data are stored, and only a limited part is useful for extracting knowledge and execution.

Distributed storage solution such as InterPlanetary File System (IPFS) through the MEC architecture will be an interesting area for exploration.
The data is not stored on the DLT itself, but the network at hand can leverage the DLT as a ledger for payment automation and/or for value exchange, enabling device storage access.

**Security:** To achieve the optimal model of IoT, security needs to be at the core foundation in the IoT ecosystem, with rigorous validity checks, authentication, data verification, that needs to be encrypted at all levels, without a solid bottom-top structure. More threats will be created with every device added to the IoT network. Introducing cryptographic hardware in the solution could accelerate cryptographic operations and offload the system from complex DLT software protocols. Protection of data and privacy are key challenges for IoT. The industry needs a compliance framework for IoT that includes hack resistance and privacy protection. This is by no means an easy task, but trade-off is made possible by the implementation of DLT technology.

**Governance:** Governance is similar to a constitution. To support the DLT community in reaching consensus on two strategic areas: The protocol guideline (the code) and incentives of the network (Economic model) to ensure long terms sustainability of the network as a whole. This is seen as a mix between human intuition and algorithmic governance and will only work if the guidelines are robust, fair and predictable. XENIRO have implemented a solution for DLT with certain aspects of democracy, based on an on-chain voting system. Execution is run within the DLT protocol that is optimized for the proposed network.

**The Blockchain (DLT) Trilemma:** Much of the innovation DLT technology has been aimed at wresting power from centralization. Unfortunately, the DLT community’s vision of a decentralized world comes at a cost. The goal for blockchain 1.0 was clear: these blockchain projects were trying to establish themselves as secure, decentralized monetary systems. In blockchain 2.0 came the scalability issue, leading projects to sacrifice either security or decentralization in order to explore scalability as a compromise.

The founder of Ethereum described this as the “Blockchain Trilemma” based on the belief that blockchain can only achieve 2 out of 3 of these traits at one time. The model is described as follows:

**Decentralization:** Defined as the system being able to run in a scenario where each participant only has access to O(c) resources

**Scalability:** Defined as being able to process O(n) > O(c) transactions

**Security:** Defined as being secure against attackers with up to O(n) resources
Syntax \( C \) refers to the size of computational resources (including computation, bandwidth, and storage) available to each node.

Syntax \( n \) refers to the size of the ecosystem in some abstract sense. With the assumption that transaction load, state size, and the market cap of a cryptocurrency are all proportional to \( n \).

The inherent problem is that by increasing the quality of any one element, one must somehow forgo some of the benefits of the other two aspects.

There are several prominent production concepts within the community to address the three trilemma principles. Projects such as Side chains (create a side network to process a specific type of transaction, that record only the beginning and ending outcomes on the network), Sharding (breaking down data into small chunks of data, where nodes are separated into groups and a specific chunk of data are processed by these groups of nodes. Later, they are reassembled and stored on the DLT). Increased block size (Forking may occur, and modifications can be made to the chain. By increasing the size, more transactions can be stored per block).

Depending on the types of solution, there are always pros and cons. At XENIRO, we believe that to achieve a balanced state (optimal point) within the trilemma (Figure 3), focusing on the DLT algorithm alone to maximize two of three qualities on the trilemma is not possible.
We need the support of external network infrastructure forces and adjustments to hardware solutions in order to break the trilemma to achieve the desired balanced state. Hence, this is where MNOs’ emerging infrastructure plays a crucial role in the DLT ecosystem, eliminating the triangular plane.

5 XENIRO Vision

5.1 The xGRID – A New Network Paradigm

In the previous chapter, we discussed some of the opportunities and characteristics where MNOs become the new valued network, DLT is the new ecosystem platform enabler, and IoT is the potential monetizer in this ecosystem. This newly created infrastructural network paradigm is called the “xGRID”. “x” represents infinity and the “GRID” refers to a new federated network, that is chained and in-sync through the 5G MEC infrastructure via the XENIRO SnapScale DLT.

The industry will accelerate the deployment of micro data centers, without further heavy investment in centralized data centers. Being positioned at the edge of the network provides blazing 5G latency performances, interworking in combination with unlimited compute, storage and networking resources through the MEC. Any IoT machines or devices onboarding the SnapScale DLT can essentially provide services and transact with any IoT devices through MNOs MEC infrastructure, where devices are equipped with the capability to “Roam” on the SnapScale protocol. We foresee xGRID in becoming the new mobile edge infrastructure, that will power the future of DLT protocols in Industry 4.0 and beyond.

We foresee xGRID in becoming the new mobile edge infrastructure, that will power the future of DLT protocols in Industry 4.0 and beyond.
The **xGRID Network**

![The xGRID Network Diagram](image)

**CLUSTER** = Cluster of MECs (Regional)

**The xGRID** = Federated Clusters (Global)

Figure 4 highlights a new envisioned network with virtualized enabled MECs, connected through SnapScale DLT confined on a local level. As more MNOs join the network, it expands to become regional/global-clusters. Finally, with a partnership through a cross-border federation framework, MECs ultimately become a network of multiple scalable clusters on an intercontinental level, making up the “xGRID” network. This will eventually constitute towards the world’s largest distributed network.

The beauty of the 5G networks is its ability to flexibly execute multiple services through super high-frequency spectrum, catering for a wide range of industry performance requirements (such as high throughput, low latency, very high reliability, and security). A capable single physical network, that provides services through separation of segregated layers via a customized logical network - that is a Network Slice (NS) sharing a common physical infrastructure. We define a network slice as a processing...
path containing all the networking functions needed to deliver a service. Network slicing enables service collaboration across network domains, cross operators and cross industries.

Self-evidently, providing this capability requires strong industry partnerships. This may come in the form of 3GPP standards and working with other networking organizations on common interfaces. This is fundamental in developing a system that is interoperable between MNOs, that can be built and operated using multi-vendor technology and can achieve global reach and economies of scale. “There is an essentially an economy of scale for Network Slicing” through service exposure. Imagine an infinite array of possibilities where we leverage the 5G NS through the MEC infrastructure, on-boarding IoT services running on the SnapScale DLT protocol, creating an extreme network that unleashes all three capabilities within the ecosystem.

**SnapScale DLT**

Figure 5 depicts how the transaction flow between IoT devices, the MEC infrastructure, with the final recipient executed on the SnapScale DLT platform. This newly refined architecture will boost DLT scalability to a new level.
**Scenario (A) in the diagram:** The autonomous vehicle needs to be charged at the Electrical Vehicle (EV) charging station. The XENIRO SnapScale DLT facilitates the transaction by allowing the autonomous vehicle to make payments automatically through a smart contract with the EV charging station, processed through a nearby MEC. This processing could take the form of device authentication, privacy encryption, and performance boost through the XENIRO ORDOS ASIC chip embedded in the MEC. Due to the weight of the transaction (Smart Contracts are categorized as heavyweights), the Distributed Ledger Smart Policy Engine (DSPE) residing in the automation platform will divert the transactions to be processed on the primary layer of the SnapScale DLT. This design intelligently segregates workloads, based on transaction type on the chain, for enhanced service acceleration.

**Scenario (B) in the diagram:** Assuming a security company offers a security surveillance service for the EV charging station requiring Nano transactions to be paid on a daily interval: in this specific instance, there is no need for smart contract deployment. Due to the nature of these lightweight transactions, DSPE will divert them to have them processed on the secondary layers of the SnapScale DLT for efficiency.

In both scenarios, we are segregating the workloads on the SnapScale through intelligent detection with DSPE, enhancing performance in extending scalability through a decentralized setting. (DSPE supports service flow detection, policy enforcement and flow based DLT transactions on SnapScale).

**Federated Network Slicing**

Federated network slices for 5G roaming extends this concept to a visited network. This technology will make it possible for an operator to provide a global IoT network service, ensuring enterprises do not need individual agreements with different operators for a global service experience.
In Figure 6, assume an autonomous taxi company (based in US) has signed up with a multimedia advertising company (based in Asia) for providing advertising services within the in-car system. Both companies are located on different continents. There is an open slot for a five minutes advertising campaign. The Media advertising company will initiate a smart contract through the MEC with the taxi company once the payment is validated on the XENIRO SnapScale DLT. The service will then be streamed through the local MEC with 5G connectivity that runs all the way, deep inside the Asian operators virtualized core network (NFV) applying specific federated network slices with guaranteed Quality of Service (QoS). This service will also be delivered through the counter-party operator’s 5G and MEC infrastructure on the other continent (US) and directly onto the system panel of the autonomous vehicle.

This network slice will be made available on both operators’ platforms, preferably with servers hosted on each other’s data centers, specifically for enterprise that want to maintain all network services across different operator footprints, which often requires inter-operator agreements. The Key business value through NS is that it enables global service offering for a multitude of industries and provides an opportunity for MNOs to address various use cases within the networked society. This is highly relevant as it exemplifies seamless service experience and control, while simplifying the enterprise and operator partnership.
Federated Network Slicing: Proof Points

In 2017, Ericsson demonstrated the concept of world’s first intercontinental 5G federated network slicing field trial together with Deutsche Telekom and SK Telecom, showcasing multiple applications use cases. In 2018, British Telecom (BT) and Verizon together with Ericsson explored the capabilities in virtualization, edge cloud computing and 5G for network slicing for mission-critical applications across continents. Huawei also published a joint whitepaper in 2017 with China Mobile, Deutsche Telekom, and Volkswagen titled “5G service-Guaranteed Network Slicing”.

These collaborative field trials have proven that federated network services are a powerful reality with viable commercial vertical opportunities. What we believe is missing concerning infrastructure adoption is merely an emerging platform with an economic model. XENIRO SnapScale DLT holds the key to the missing platform with the tokenized economic principle through:

- Opening up an exponential level of business innovative with this distributed architecture.
- Reduced transaction fees (avoid lengthy clearing and settlement processes).
- Elimination of currency risks (for international services).
- Exploring the economies of scale in Network Slicing through MNOs investments in 5G & NFV.
- SnapScale in MEC acts as an aggregator for processing millions, if not billions of IoT transactions either locally or globally, ideally becoming a profit center in MNOs network.
- Opening up a world of decentralized multi-applications on DLT, delivered at the edge.
XENIRO’s vision is to empower MNOs in leveraging their existing network infrastructure, combined with DLT technology to expose renewed innovation in the telco space. This is about unleashing extended value out of the current infrastructural investment in 5G and should not be considered just another generation of a renewed “connectivity pipe”.

5.2 Applicable DLT Use Cases

DLT-based applications are disrupting all major industries today. Let’s examine some of the use cases and opportunities.

(A) IoT: Electric Charging (Autonomous Vehicle + Drones)

The market for EVs has been growing steadily over the last decade, and the prospects are good for stronger growth in the fields of light-duty consumer vehicle / commercial vehicle/drone electrification. One of the global drivers is the renewed appetite at all levels of government for clean energy. Thus, the market requires an available charging infrastructure that is fast and convenient. The EV charging ecosystem is very complex, and most projects need strong partnerships between both public and private stakeholders to deploy necessary infrastructure. Critical stakeholder groups in the EV charging market include electric utilities, equipment, software and services vendors, MNOs, governments and non-governmental organizations. With such complexities, XENIRO SnapScale DLT could automate transactions on the ledger between stakeholders as depleted in (A) Between power plant utility providers (B) Vehicle to EV Charging station (C) Drone to Electric Charging station through Smart contracts and Micro / Nano transactions. Whether it is B2B or B2B2C, each level of transaction is simplified by smart contract automation through the MEC, serving low-latency and high-bandwidth requirement. All data and transactions are safely stored on the decentralized SnapScale DLT, with MNOs infrastructure at the center in processing these transactions (Figure 7).
(B) **IIoT: Supply Chain Management**

Majority of the supply chain stakeholders experience challenges to maintain a holistic view of the supply chain networks due to data silos and interoperability. In today’s complex manufacturing ecosystem, participants often do not know one another and lack visibility into each other’s data and activities where “Trust” becomes a significant concern.

The supply chain has grown in scope and scale concerning complexities when it comes to managing multiple suppliers across multiple industries. The real promise DLT brings to IoT is to automate trusted services through codes and intermediating the flow of data. Consider the opportunity for disparate manufacturers, brands, service providers, advertisers, insurance companies, energy providers, etc. to leverage each other’s platform to extend and improve upon their services.

With the introduction of DLT technology, that offers a decentralized approach to data management and sharing of information, whereby the access of data for all stakeholders becomes trusted, adding aspects of autonomy and transparency through this innovative approach, that ultimately achieves security and efficiency.
Some of the major benefits through DLT can take the form of: (A) Real-time tracking, time-stamping, autonomous processing where events can be audited in real time: this creates transparency and usage of shared data sources by using data lakes which gather data through the whole supply chain (B) Self-executing contracts through smart contract deployment: this is when defined events are executed autonomously when the parameters are fulfilled and agreed upon (C) Minimize the involvement of intermediaries (E.g. Insurers, banks, brokers) in simplifying the supply chain process (D) Speed-up process in onboarding new partners and vendors through assigning newly created digital IDs (E) Indestructible record that is tamper-proof and guarantees the integrity of information.
The use case demonstrated above (Figure 8) depicts a supply chain scenario involving three parties.

(A) The primary producer

(B) The manufacturing subcontractor of the primary producer

(C) Logistics vendor

A smart contract is deployed between the primary producer (A) and its manufacturing partner (B). With this proposed solution, data is written onto the XENIRO SnapScale DLT synced through the MEC distributed architecture. When the manufactured goods are ready for shipment, a new smart contract is initiated between the manufacturing partner (B) and the logistics vendor (C). Based on the agreed terms and conditions, the finished goods will be delivered to the primary producer (A) on an agreed date.

In the example above, the primary producer (A) will create smart contracts of all the critical stakeholders in its value chain. This could include the identities of who will be part of the SnapScale DLT and can participate in a production, shipping, customs clearance, warehousing scheduling and so on. These sets of identities are granted access to read and modify for a complete end-to-end service.
XENIRO’s solution resolves a variety of current supply chain challenges on the SnapScale DLT via MEC. With the creation of a common shared ledger, that automates with smart rules in deploying dynamic contracts, and ledger entries. SnapScale DLT is deemed to unlock the full potential in supply chain economics.
(C) Multiple Decentralized Applications (Mixed Reality)

The market for Virtual Reality (VR) / Augmented Reality (AR) is growing at a rapid pace, many institutions are starting to integrate VR in corporations, educations and the public may even want this service in their homes. Incorporating immersive technology, deepens learning experience and expands the reach to the higher population, which represents a colossal market-driven opportunity. The example below (Figure 9) demonstrates a scenario where a museum creates a decentralized VR / AR application on the XENIRO SnapScale DLT where: (A) VR-to-Home (B) VR-to-School (C) Museum

![Diagram of decentralized VR applications](image)

The Museum deploys a smart contract with multiple (A) Homes (B) Schools globally or locally to create a VR excursion of their museum streamed directed to their homes or classrooms. This makes the cost of learning more economical and complementary in adopting VR technology. Transactions between the VR-to-Home or VR-to-School can take place directly on the SnapScale DLT through an automated smart contract. The VR contents will be processed instantly via the DApp on the MEC, with reduced latency through 5G, for an enhanced QoS experience. This use case could potentially be extended to VR in entertainment, industrial enterprises or even medical trainings with groundbreaking DApps, integrating tactile Internet & MEC openness for an immersive experience. Eventually, it will enable the provision of a real P2P valued service at scale, with an application-centric business model.
In this section we will be assessing the details of the disruptive XENIRO solution at the core of this architecture. This is divided into three critical complementary interworking components:

- XENIRO Automation Platform (XAP)
- XENIRO SnapScale DLT
- XENIRO ORDOS ASIC

### 6.1 XENIRO Automation Platform (XAP): Multi-Access Edge Computing (MEC)

XENIRO’s Automation Platform is a container-based orchestration platform that is trusted, policy-driven, supporting the deployment, diverse workload, orchestration and governance for SnapScale DLT. This platform enables enterprises and developers’ communities to accelerate multi-decentralized application adoption, taking advantage of speed, performance, scalability and cost effectiveness while ensuring operational governance and compliance for mission-critical IoT application.

XENIRO XAP is essentially a compute system that includes containers, microservices, and SnapScale DLT functions as a “Serverless Architecture”. A key factor with XAP is that with a decentralized architecture, it can achieve resilience through an autonomous subsystem. If a specific MEC is suffering a temporary outage, certain local areas or regions, their nearby MEC clusters should become the autonomous subsystems, without any impact to the XAP. DApps running on top of SnapScale DLT are lightweight and can be migrated easily with services being executed on demand. The main idea is to create a Zero-Touch operation system with XAP (See Figure 10).

At the heart of the XAP architectural stack is the hybrid storage architecture (Distributed + Decentralized file systems) without the current silos of data. It is decentralized and distributed with advanced cryptography hash for added security. The XENIRO Virtual Machine (XVM) serves as a runtime environment for the smart contracts, enabling transaction automation, handling the internal state of the network (also known as a transaction-based state machine). XVM also handles account information applicable to addresses, balances, transaction fees and block information that is immutable, deterministic, operational and verifiable. Every XAP nodes serve as a connection point for all members within the consortium, and every node in the SnapScale DLT runs on XVM in maintaining consensus across the DLT, allowing for smart contract execution.
Residing in the SnapScale DLT is a newly defined “Distributed Ledger Smart Policy Engine” (DSPE), a critical XAP component that allows for monitoring & service segregation in optimizing the resource utilization on the DLT protocol. It works as a highly programmable policy engine that supports service routing on the SnapScale DLT based on transaction type (token charging rule) to enhance Transactions Per Second (TPS) performance and is served dynamically in real time. DSPE service integrity is crucial, in its role to ensure that transactions can operate efficiently under heavy capacity utilization. Other DSPE features include: XENIRO ORDOS Processor integrator (interworking with the ASIC chip), Zero-Knowledge Proof parallel job distributor (for privacy), Oracle information retriever (agent for real-world occurrences), XAP state monitor, Smart contract registry finder and Reinforcement Learning (RL) processing, that integrates seamlessly with the XENIRO stack solution.

At the very top of the XAP stacks are the DApps, (DLT enabled websites/platforms) that utilize smart contracts (acting as a logic brick) to execute commands and retrieve information from the SnapScale DLT. This is an environment where the developer community creates a variety of DApps, ported through the underlying MEC infrastructure with QoS in providing a flawless user experience.
Figure 11 on the left shows an Ethereum based smart contract infrastructure. With its wide range of tools made for and by DevOps, it is relatively well-defined. However, all contracts in their network require “gas”, and all nodes need to execute simultaneously, utilizing a hefty amount of energy.
Currently, adoption of smart contracts is limited to only a few, any users without the knowledge of programming will not be able to access it as they have to code in the terms and conditions. Further insight is needed to make all the edits of the system and update the code whenever terms are changed. While Ethereum applies its smart contracts on the DLT, XENIRO is looking to deploy the code off the DLT, so that developers can interface with by way of a RESTful API with various programming languages of their choice with a variety of SDKs.

An IoT application can be native business logic or smart contract virtual machine. XAP allows these applications to coexist and run in the same instance of the DLT network, thus segregating the core system from the application and simplifying the development.

XENIRO is looking to create an environment for ease of integration with MNOs or enterprise IoT existing systems, thereby deploying business logic solutions without having to start from scratch, adapting business ready existing systems to the SnapScale through XAP. The aim is to provide the most enterprise/developer friendly platform on the market.

Scalability is the most critical aspect of XENIRO’s decentralized applications, due to the nature of the IoT characteristics. In the emerging IoT era, applications that require autonomy, low-latency, and hefty bandwidth are suited in deploying smart contracts through the XENIRO architecture (MECs in combination with XAP are designed specifically to handle these types of workloads).

XAP will comply with ETSI defined API solutions, incubating an ecosystem that will allow for community development of multiple applications such as facial recognition, drone-related services, mixed reality, real-time video streaming, autonomous vehicle and vertical industry services.

**XENIRO MEC Infrastructure**

According to the current market projection, there is an estimate of 6.5 Millionxiv telecom towers installed globally. This number will continue to ramp-up with 5G adoption. Assuming that each radio tower is paired with a MEC. This implies a potential of 6.5 Million MEC nodes around the world to serve billions of IoT devices. If we think about the current general DLT industry as a whole, nodes are operated by individuals and lack the infrastructural characteristics (resilience, flexibility, security, latency, bandwidth) of an MNO infrastructure. Figure 2 shows node differentiation between a public node (Ethereum a popular example) compared with MNO-operated MEC nodes, with distinctions regarding compute, storage and networking capabilities when processing IoT transactions. Public DLT nodes are not “one size fits all” solutions, and not applicable for adoption in all industries.
<table>
<thead>
<tr>
<th></th>
<th>Ethereum</th>
<th>MEC + SnapScale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nodes</strong></td>
<td>Current 15K~</td>
<td>6.5M+ MEC Nodes</td>
</tr>
<tr>
<td><strong>Computing Power of Node (Average)</strong></td>
<td>PC / Workstation</td>
<td>12 two-way blade servers</td>
</tr>
<tr>
<td><strong>Infrastructure Provider</strong></td>
<td>Personal</td>
<td>Enterprise</td>
</tr>
<tr>
<td><strong>Access Type</strong></td>
<td>ADSL, FTTx, Cable</td>
<td>4G / 5G</td>
</tr>
<tr>
<td><strong>Node Reliability</strong></td>
<td>High</td>
<td>Extremely High</td>
</tr>
<tr>
<td><strong>Node Availability</strong></td>
<td>Low</td>
<td>99.999%</td>
</tr>
<tr>
<td><strong>Node Security</strong></td>
<td>Low</td>
<td>Extremely High</td>
</tr>
<tr>
<td><strong>TPS</strong></td>
<td>Slow</td>
<td>Ultra Fast</td>
</tr>
<tr>
<td><strong>Bandwidth (Average)</strong></td>
<td>100 Mbps–1Gbps</td>
<td>5G with 20+ Gbps</td>
</tr>
<tr>
<td><strong>Transaction Latency</strong></td>
<td>Very High</td>
<td>1ms air latency with E2E latency at 5ms with 5G</td>
</tr>
<tr>
<td><strong>IoT devices / Sq KM</strong></td>
<td>N/A</td>
<td>1 Million with MEC</td>
</tr>
</tbody>
</table>
There are 3 service layered MEC deployment stacks from an MNO perspective (Figure 13), where DApp services can be constructed from a set of modular components that are assembled in ways to create different experiences across the MNOs network.

**NFVi Solution (I):** This is where MNOs infrastructure is evolved through applying standard open IT virtualization technology. That is split into distinct layers. The HW and infrastructure SW required to run the platform that works with virtual servers and bare-metal, together with VMs, hypervisors. The Network Function Virtualization Infrastructure Manager (VIM) that is made up of VMs and hypervisors, and the Virtual Network Functions (VNFs) for telecom-grade applications that delivers specific network functions such as routing, mobile core, caching, etc. Residing on top of the VIM is the ETSI defined service APIs\textsuperscript{xv} (GS MEC 009, GS MEC 010-2, GS MEC 011, GS MEC 012, GS MEC 013) exposing interoperability with MEC + DApps within the VM. The XENIRO XVM with SnapScale DLT algorithm essentially becomes a VNF application within the NFV framework.

**VM Solution (II):** Very similar to NFVi solution (I) except that XAP becomes a platform hosted in MNOs MEC, sharing infrastructure resources, that is interoperable with ETSI API. XAP supports XVM through smart contract deployment for DApps.
**Bare-Metal (III):** A bare-metal option, whereby XAP becomes the hosted OS for DLTs allowing various types of community built MEC applications, to be deployed through a VM or containerized architecture, in conjunction with XVM for smart contracts.

These integrated solutions provide MNOs with the flexibility for SnapScale DLT deployments that opens up a host of community-driven DApps, as an extension to existing MNOs VNF centric applications, with economies of scale.

*Federated MEC container orchestration*

For its ecosystem, XENIRO aims to create a federation through the interconnection of Global and Regional MECs on the xGRID network (Figure 14). This requires creating a mechanism for multi-cluster geographical replication orchestration framework and opens up opportunities for DApps to be orchestrated globally via cross federated MEC clusters in pursuit of efficiency, reliability, and performance. For instance, a given DApp deployment can be kept consistent between multiple MEC clusters, and different clusters can share service discovery so that a back-end resource can be accessed from any cluster. With built-in controllers, it assists in providing high availability of crucial fabric components like processing smart contracts with their fabric peers. If somehow a container is out of service, another one will be created automatically, in other words, zero downtime for DApp fabric containers in MECs.
Apart from serving as a solution for deploying DApps that run on SnapScale DLT, containers are highly complementary in many aspects that share some essentials characteristics with SnapScale DLT such as (1) **Decentralization**: containers are distributed and decentralized, shifting across environment as DApp demand dictates. (2) **Scalability**: Highly scalable (3) **Fault-tolerance**: If one DApp fails, the rest is always available to ensure continuity. These important shared traits create some very compelling use cases, becoming a valued driver for mainstream adoption in the world of DLTs.

### 6.2 XENIRO SnapScale Hybrid DLT

DLT is a database that is distributed across several nodes or MECs. Each MEC replicates and saves an identical copy of the ledger in the network and updates itself automatically. Therefore, no ledger is maintained by a central entity. Blockchains are one type of DLT that is distributed and managed by a P2P network. The structure of the blockchain makes it distinct from other kinds of distributed ledgers and Data on the blockchain is grouped together and organized into blocks. The XENIRO SnapScale DLT consists of two types of data structures, Blocks, and Graphs.

**Blocks | Layer I – Main Chain**

A block is considered to be the prime blockchain data structure (Figure 15). A blockchain data structure is mainly hash pointer based and involves blocks as the main data structure. The different blocks in a blockchain are identified with the assist in the block header, which is generated cryptographically with the support of the hash algorithm. Blocks are a container data structure that helps in bringing together of transactions to be included in the ledger. Their structure includes a header and a long list of transactions. Their header consists of (A) Index (B) Hash (C) Previous hash (D) Number of Transactions (Tx) (E) Timestamp (F) Nonce. These are the summary of transactions performed in the block. This flat, sequential nature of blockchains is what gives us the ability to trace back any block written in a ledger. With blockchain, every block references the one before and including its hash, which leads to bottlenecks when too many transactions requests are being made.

---

**Figure 15**
DAG | Layer II – Side Chain

DAG\textsuperscript{xvi} is a different type of data structure (Figure 16), it is an implementation of graph, and it allows the networks using it to circumvent some of the blockchain’s most daunting limitations. It uses a topological ordering/sorting sequence. In DAGs, all the nodes are pointed in the same direction, and no element can reference back to itself. As in a tree-like structure, there must be unique paths between every two nodes. DAG powered networks allow appending parallel nodes as long as everything flows in the same direction. The advantages of DAG are that there are no blocks, each new transaction cannot be confirmed unless you confirm two previous transactions. With DAG technology, the higher the number of past transactions, the more prior transactions are available to confirm the current transactions. In theory, DAG may be faster, as it is designed to complete the length of the sequence in a short space of time. There is theoretically no limit on transaction throughput as transactions are directly linked rather than grouped or serialized on a single lane. The technical design also allows a broader range of algorithms which could be applied, and therefore, with expanded flexibilities.
XENIRO SnapScale combines both a block and a graph structure. Reason being is the belief that assorted IoT devices will require various types of payment transactions to avoid congestions on the main chain. For example, any IoT Nano-transactions below a certain token value threshold, will be executed on the DAG platform, and transactions that require smart contracts and token value above a higher level of limit will pass through the main chain. Figure 17 below depletes a diagram on the design of SnapScale DLT.
Two-Way Peg

A sidechain is defined by a custom “rule-set” and can be used to offload computations from another chain. Individual sidechains can follow different sets of rules from the main chain (Layer I), which means they can be optimized for applications that require extremely high speeds. Sidechains should simply be understood as a discrete graph that is linked to the main Block applied through a “Two-way peg”xvii. The functionality of sidechain holds significant potential for the enrichment of the capabilities for SnapScale DLT. In this case, DAG acts as a sidechain when an IoT device on the main chain has to send funds to an output address. Once the tokens are in the output address, they are locked-in. This means that the IoT device is no longer able to use the tokens.

To ensure increased security, communication is sent across the main chain and sidechain and a waiting period is permitted after the IoT device tokens have been moved to the output address. Once the waiting period elapses, the token is released to the sidechain. The IoT device is then able to spend the tokens on the sidechain. When moving from the sidechain to the main chain, the machine sends the tokens from the sidechain to an output address where they are locked. Once the waiting period is over, an equivalent number of tokens is transferred to the main chain. This acts as a two-way synchronization between the two-hybrid DLTs.

The sidechain takes many forms of benefits such as: (1) DAG sidechains are independent of the main chain, they are firewalled and responsible for their own security without major risk for the integrity of the main chain (2) DAG is known for scalability through parallel transactions in its own nature, with DAG being a layer II scaling that allows transactions to be conducted off-chain. This can be scaled further with IoT and takes pressure off the main chain, allowing it to further accelerate transactions (3) Supports two way pegged assets (side chains issue an asset that is backed at a deterministic exchange rate to the main chain assets) with interoperability (4) The option to include a federated sidechain to add nodes in-between the main chain and side chain through consensus.

Consensus Mechanism | Delegated Proof of Stake (DPoS)

Consensus mechanism is the soul of the DLT network. It is a fault tolerant mechanism that is used in the system to achieve the necessary collective agreement on a single state of the network. To put it simply, it is a dynamic way of reaching consensus within a group of computer nodes.

One of the main consensus characteristics of the XENIRO SnapScale is the Delegated Proof of Stake (DPoS)xviii. This is a two-tier governance structure that has been proven in Steem and Bitshare (Larimer 2014)xix. In 2018, a new version of DPoS was included with BFT (Byzantine Fault Tolerance) to enhance both the performance and governance on the chain.
This was implemented in EOS and is notably seen as one of the most decentralized, efficient and fastest distributed consensus ledgers in the industry. This consensus mechanism utilizes a democratic framework to offset any effect related to the full centralization of network nodes.

In DPoS, the stakeholders elect what are known as witnesses (In this case, MNOs selected MEC nodes as candidates). The stakeholders allocate their token to witnesses as their vote. The more tokens they have, the higher their voting powers. Stakeholders remain in control and operate the network properly through the witness production of blocks in avoiding penalties. Stakeholders can vote for as many witnesses as they wish so long as 50% and more of the stakeholders believe that adequate decentralization has been achieved. The witnesses are responsible for adding blocks (process and validate transactions) to the DLT and are rewarded with tokens on the platform. If the witness fails to produce a block at the allocated time, they may be voted out by stakeholders.

DPoS uses a reputational system and real-time voting to elect a panel of witnesses. At every t time interval, the witnesses re-shuffle and take turns adding the blocks according to the new ordering. The number of witnesses on the SnapScale platform is limited to 101 witnesses (or equivalent to 101 MEC nodes worldwide) to validate transactions. Thus, in order to add blocks and receive rewards, MNOs have to compete on a worldwide level to be in the top 101 witness list. What this essentially means is that 101 MEC nodes belonging to the MNOs will be voted to become witnesses on the XENIRO SnapScale DLT.

The witness list will be ranked according to the number of votes each witness receives. Witnesses have a big responsibility to ensure the integrity of the SnapScale DLT platform. MNOs who wish to become an elected witness can increase their reputation by making contributions to the network. The abstract protocol for DPoS includes the following: (A) Proposed block (B) All participants acknowledge block (Pre-commitment) (C) All participants acknowledge when ⅔+ have sent them pre-commitments (Commitment) (D) A block is finalized once a node has received ⅔+ commitments (E) Unanimous agreement on finality is guaranteed unless ⅓+ are bad and evidence of bad behavior is available to all.

Delegates on the other hand, are elected similarly to witnesses through stakeholders. However, delegates are responsible for maintaining the network and can even propose changes to the network parameters. Changes can be in the form of: block sizes, block intervals, fees paid to witnesses, transaction fees. Once these changes have been submitted, it is then up to the stakeholders to decide whether or not the proposed changes should be implemented.

This method of approval ensures that the delegates do not have power over the system and cannot make changes on the DLT without the approval of the stakeholders. The changes to the network parameters can only be made by the stakeholders, with the primary aim being to institutionalize a self-governing model within the MNO space.
DPoS (Figure 18) adopts the idea from many traditional governance models but is ultimately far more flexible and transparent. DPoS is the driving power behind the main chain within the SnapScale DLT. Decentralization in DPoS has a cost, both economically and in terms of performance. However, the design of this consensus opts for semi-decentralization in exchange for scalability, which is far more suited in the IoT domain and indeed more pragmatic.
Zero-Knowledge Proof (ZKP)**

As IoT becomes further automated, privacy and data protection will become paramount. If multiple entities join a DLT network, all entities can access data in the network, especially those with sensitive business intelligence that they want to keep private. Applying ZKPs is an ingenious way of ensuring privacy on the SnapScale DLT. Rather than recording all the data from IoT transactions, ZKP allows entities to store only the proof of the transaction on a node. They can keep the sensitive data to themselves, while still maintaining confidence in a connected record of provenance.

*A zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that something is true, without revealing any information apart from the fact that this specific statement is true.*

To simplify; zero-knowledge proofs (ZKP) let you validate the truth of something without revealing how you know that truth or sharing the content of this truth with the verifier. This principle is based on an algorithm that takes some data as input and returns either ‘true’ or ‘false’. Zero-knowledge proofs have been generating a lot of interest lately, mainly due to their potential for enhanced privacy and security in DLT applications. The three main characteristics of ZKP must satisfy these criteria:

1. **Completeness**: if the statement is true, the honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.
2. **Soundness**: if the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.
3. **Zero-knowledge**: if the statement is valid, no verifier learns anything other than the fact that the statement is true. In other words, just knowing the statement (not the secret) is sufficient to imagine a scenario showing that the prover knows the secret. This is formalized by showing that every verifier has some simulator that, given only the statement to be proved (and no access to the prover), can produce a transcript that "looks like" an interaction between the honest prover and the verifier in question.

The first two of these are properties of more general interactive proof systems. The third is what makes the proof “zero-knowledge”.
The Model

To demonstrate this in a mathematical computation model, we can use the most common example such as a Turing machine. Let $P, V$ and $S$ be Turing machines. An interactive proof system with $(P, V)$ for a language $L$ if for any probabilistic polynomial time (PPT) verifier $\hat{V}$ there exists a PPT simulator $S$ such that:

$$\forall x \in L, z \in \{0, 1\}^*, \text{View}_\hat{V} \left[ P(x) \leftrightarrow \hat{V}(x, z) \right] = S(x, z)$$

Where:

$$\text{View}_\hat{V} \left[ P(x) \leftrightarrow \hat{V}(x, z) \right]$$

is a record of the interactions between $P(x)$ and $\hat{V}(x, z)$. The prover $P$ is modeled as having unlimited computation power (in practice, $P$ usually is a probabilistic Turing machine). Intuitively, the definition states that an interactive proof system $(P, V)$ is zero-knowledged if for any verifier $\hat{V}$ there exists an efficient simulator $S$ (depending on $\hat{V}$ ) that can reproduce the conversation between $P$ and $\hat{V}$ on any given input. The auxiliary string $z$ in the definition plays the role of “prior knowledge” (including the random coins of $\hat{V}$). The definition implies that $\hat{V}$ cannot use any prior knowledge string $z$ to mine information out of its conversation with $P$, because if $S$ is also given this prior knowledge then it can reproduce the conversation between $\hat{V}$ and $P$ just as before. Here, the example above is a mathematical definition given is that of perfect zero-knowledge$^{xxi}$.

To understand the ZKP methodology in a Machine to Machine transaction scenario, we can simplify this by applying the following example:

Assuming Machine A puts 100 tokens in a smart contract with Machine B. Whereby Machine B is paid to do a particular task, on the completion of which, Machine B will get the 100 tokens based on the smart contract. This gets complicated when the tasks that Machine B has to do are multi-layered and deemed confidential. Suppose a smart contract has been entered with Machine A. Based on the terms of the contract, Machine B will only receive the payment if task A1, A2, A3 is completed. What if Machine B doesn’t want to reveal the details of A1, A2, and A3 because they are highly confidential to your company?

What ZKP does is that it proves that those steps have been executed in the smart contract without revealing what those steps are. Its sole purpose is to protect your company’s privacy and security. It only reveals certain parts of the process without revealing the complete process to prove that you are honest about your claims.
6.2 XENIRO ORDOS ASIC

MEC servers in general follow a standard x86 ISA (Instruction Set Architecture) CPU-based architecture with the aim of processing and executing multiple tasks effectively. The x86 design used to dominate compute intensive workstations and the cloud computing segments. ASICs (Application Specific Integrated Circuits) on the other hand, are silicon chips that are designed for a very specific purpose, that is created to perform a specific function effectively. They are targeted for high performance computation that is thriving in popularity. Deemed as the next wave of chip transformation, thereby becoming a natural choice in boosting system performance for DLTs.

XENIRO Acceleration Device (XAD) is a hardware powered by ORDOS ASIC and embedded as part of the MEC server architecture, for performance acceleration, with an added layer of fortified security on the SnapScale DLT. The main motivation behind the ORDOS ASIC solution design is based on the following logics:

- ORDOS ASIC provides dedicated computational resources with precise timing control in boosting system performance (throughput & scalability), without any trade-off within the “Blockchain Trilemma”.

- It includes an advanced built-in accelerator block (E.g: Zero-Knowledge Proof, ECC, SHA-3) that will become mainstream. ORDOS ASIC will be fully optimized to integrate seamlessly with SnapScale DLT.

- ORDOS hardware provides a Trusted Execution Environment (TEE) ensuring that data stored, processed are protected in a safe and trusted environment.
ORDOS ASIC will be fully optimized to integrate seamlessly with SnapScale DLT

For ORDOS ASIC to co-work with SnapScale DLT, it requires the support of DSPE (Distributed Ledger Smart Policy Engine) in compiling multiple tasks from SnapScale DLT. Figure 19 demonstrates the process flow of DSPE forwarding & assigning the computing/memory intensive tasks, proceeding towards the ORDOS ASIC.
**ORDOS ASIC Architecture**

XAD (XENIRO Acceleration Device) is a system board level device, with embedded ORDOS ASIC (Figure 20). The core processor of ORDOS is designed based upon the classical Von Neumann architecture. For security reasoning, the on-chip memory/storage will be implemented either on-die (SoC) or in-package (SiP). Dependency will be the memory/storage density requirements. ORDOS ASIC design is quarantined into two areas, the secure area (highlighted in green) and the non-secure area (highlighted in yellow). The secure area is further protected from both hardware and software design, and only accessible under an authorization mode.

A secure RAM is provided as part of memory space, it is highly secure and can be used for critical data storage, for instance, a temporary private key. The secure RAM contents will be erased immediately, as soon as any hardware or software intrusion activities are detected. Additional hardware functioning blocks (generic interface, clock distributor, power management, system service) are in the non-secure area, although they are critical to chip functionalities, but not significant to the overall system security.
A high-speed interface is required to bridge the communication protocol between SnapScale DLT and ORDOS ASIC. There will be two embedded Direct Memory Access (DMA) for fast data exchange from various internal accelerators to the external high-speed interface. AHB, APB and AHB/APB Bridger are on-chip bus components that are part of the AMBA standards from ARM.

**ORDOS Core Features**

Three main features highlighted in Figure 21.

![Figure 21](image)

**(A) Dedicated Encryption / Decryption HW accelerators for system performance boost:**

DLT scalability is measured in Transactions Per Second (TPS) that is dependent upon (1) The time is taken to put a transaction on the block or the block generation rate (2) The time taken to reach a consensus through the algorithm calculations in executing smart contracts or issuing transactions that involve complex mathematical puzzles. Unlike conventional blockchain solutions, XENIRO has developed a mechanism where most of the workloads are processed inside the MEC server (x86 ISA CPU), x86 CPU
are naturally designed to handle multi-tasks scheduling/threading management or virtualization, but not for dedicated advanced mathematical operations. With millions of connected devices, a server node must possess the capability to handle a sudden surge or burst of transactions during peak periods. The traditional solution to solve this problem is to scale-up or scale-out server resources. Thus, the most economical solution is through the adoption of ASIC architecture.

The ORDOS ASIC chip consists of various built-in hardware accelerators that coordinate with the SnapScale DSPE to accumulate a pool of workloads, and accelerate these tasks (Hash, RSA, AES, ECC, etc.) to achieve efficiency.

The communication protocol between MEC and ORDOS ASIC will be delicately designed in minimizing the communication overhead, while maximizing the throughput.

(B) Hardware ZKP Accelerator (Privacy protection without performance impact)

With privacy protection for enterprise level security, XENIRO will adopt ZKP functions as an option for each IoT transaction or smart contracts. This will mask every communication carried out between a prover and a verifier with acceleration. The performance of zk-SNARKs as of today is not yet qualified for commercialized adoption. XENIRO will implement a ZKP masking encryption service on the SnapScale DLT, with the ability to distribute the tasks across the MEC clusters and embed the ZKP accelerators as dedicated hardware. This process will involve the SnapScale scheduler (DSPE) accumulating the ZKP shielding to a task pool, with defined parameters, before ORDOS ASIC completes the tasks and transport it back to SnapScale DLT. For periods of short bursts with peak transactions, DSPE will automate and prioritize workloads. In the long run, the intention is to include implementation of multi-core/parallel processing capabilities onto the ORDOS ASIC.
(C) **Hardware based security reinforces system robustness**

Current security functions embedded on the ORDOS ASIC include ORDOS ID register, Secure RAM, OTPs (One Time Programmable), TRNG (True Random Number Generator) Secure BootROM allowing for a reliable security foundation. In combination with other advanced accelerators executed by ORDOS, namely RSA, ECC, AES, SHA-3, ZKP, etc., SnapScale DLT will be transformed into a very powerful TEE provider for decentralized IoT applications. In the following section, we will use XAD life-cycle as an example for demonstrating the value and highlights of TEE. The implementation will pass through 4 stage cycles:

**Manufacturing Stage**

A unique OID (ORDOS ID) will be programmed into the ORDOS ID register. The OID hash will also be recorded into an “OID” whitelist. These lists can be accessed by MEC nodes.

**Deployment Stage**

ORDOS shares the workload with MEC servers, where initial authorization will be processed with public key cryptography (RSA or ECC), followed by a public key exchange protocol, such as Diffie Hellman to obtain sharing keys for both parties. ORDOS then uses symmetric encryption like AES to transfer the OID to SnapScale DLT, that will perform checks against the OID hash digest, from the “OID whitelist” in validating ORDOS device identity.
Servicing Stage

As soon as ORDOS is authorized and deployed, the TEE-based hardware is constructed. SnapScale DLT is capable of virtualizing the ORDOS chip as an online TEE service towards any DApps (e.g. ZKP shielding, SHA2/SHA3, HMAC authorization, RSA or ECC key generation, Random Number Generation, Secure data storage/exchange, etc.). Also, the Secure BootROM (in which public key would be hardcoded) on-chip will provide an online secure firmware update (signed by the private key) as deemed necessary.

EOL (End-Of-Life) Stage:

During the in-service stage, XAD may malfunction, and in such case, the relevant OID would be automatically registered into OID “black-list”. Furthermore, with the consensus algorithm on the SnapScale DLT, any node behaving erratically or deemed malicious, will be eliminated from the network, and the attached OID will be registered directly into the “OID Blacklist”, thus preventing the malfunctioned or compromised XAD/ORDOS being redeployed back into service.

In conclusion, the ORDOS ASIC plays a critical role interworking with both SnapScale DLT and MEC, that supports three important traits through: (A) Enhance performance on both scalability and throughput (B) Provide privacy protection without consuming systems resources (C) Hardware-based TEE for security control.

XENIRO will introduce a family of XAD hardware, evolving from utilizing generic market components through to an in-house ASIC design. This is categorized based on MEC node types as shown in Figure 22.

XENIRO will implement a ZKP masking encryption service on the SnapScale DLT, with the ability to distribute tasks across the MEC clusters, and embed ZKP accelerators as a dedicated hardware
<table>
<thead>
<tr>
<th>XAD Category</th>
<th>ORDOS Version</th>
<th>XAD Functions</th>
<th>Node Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>XAD.0</td>
<td>MCU Based</td>
<td>SHA-256/512 AES/RSA-2048</td>
<td>Generic Node – PoC and Initial deployment</td>
</tr>
<tr>
<td>XAD.1</td>
<td>ORDOS G-I</td>
<td>SHA-256/512 SHA-3 AES/RSA-4096 ECC</td>
<td>Mid sized Node, ORDOS G-I based (Supporting small to medium scale deployments)</td>
</tr>
<tr>
<td>XAD.2</td>
<td>ORDOS G-II</td>
<td>Multi-Core Processor and / or HW Parallelization SHA-256/512 SHA-3 AES/RSA-4096 ECC ZKP Accelerator</td>
<td>Super Sized Node, ORDOS G-II based (Supporting mass scale deployments)</td>
</tr>
</tbody>
</table>
Success in the digital era will come from the combined and collaborative efforts of business ecosystems more than from the controlled efforts of individual companies. Mindsets require a certain level of re-engineering, as the world becomes even more connected or face isolated in time. Every business exists in multiple ecosystems. The challenge is to decide how your organization will mediate, survive and thrive in these ecosystems.

With over 7 billion people and more than 20 billion devices connected to the internet by 2020, interconnection will create an ecosystem full of challenges and drastic changes. To stay competitive and relevant, MNOs and DLT communities need to transform relationships with their various partners and providers to become a highly functional ecosystem, in reaching their infrastructural potentials within their domains.
This is what XENIRO sets out to achieve on day one. To create an open IoT DLT infrastructure that is interwoven, dynamic, collaborative and inclusive, allowing all members of the community to demonstrate their value through participation and contribution in creating a win-win ecosystem.

The DLT ecosystem today is extraordinarily vast and comprehensive and has attracted the attention of developers, entrepreneurs and, industry opportunists. With the XENIRO infrastructure, we are building a new platform that is collectively owned by all the participants in the network. Ranging from multiple developer communities, MNOs, Federated MNOs and enterprises coming together that previously operated in a siloed model and will now communicate and collaborate within this space. One of the main focuses of our ecosystem is to move the IoT business logic out of the enterprises and into the composite ecosystem layer. This will allow all participants to reach agreement in a way that is transparent, trustworthy and generates value to all.

7.1 Ecosystem Partners

No single entity can unlock the potential on its own, which is why XENIRO is building a DLT ecosystem to provide access to accelerate this vision. The aim is to deliver value to all stakeholders and solidify an ecosystem benefiting the whole community. Open-source innovation incubates innovation, and DLT is no exception. MNOs can start contributing to the open source community and establish their influence and get their voice heard to ensure their capabilities are being implemented into the network at the edge. Having the right platforms and tools available will also be an integral part of the 5G platform infrastructure and will be a perfect opportunity to further innovate through open source technologies. Creating a strong community will be a vital building block within this ecosystem that includes MNOs. Supporting business growth in all directions.

The XENIRO ecosystem is partitioned into various layers. At the fundamentals, we have the MNOs offering a broad base of their emerging infrastructure that is incentivized to work together democratically. SnapScale DLTs can fundamentally transform ecosystems by leveraging digital assets, also known as tokens, where an entity is entitled to a service or a product on a platform. Tokens are used to track and monetize transactions, but they are also a great tool to materialize the governance rule as an equilibrium amongst this autonomous consortium, through shared values with transparency.

The tokens will be the fuel running inside this incentivized ecosystem platform, powered by multiple stakeholders. This, in turn, propagates a network effect, laying a foundation for governance that is future proof, while maintaining immutability within the xGRID network.
XENIRO’s ecosystem (Figure 23), is centered around what we called a multi-sided platform. In this ecosystem stack, MNOs are a powerful catalyst with their core infrastructural assets. XENIRO, on the other hand, is the platform vehicle that facilitates connection, coordination, and collaboration with the rest of the open community in fully utilizing the complete ecosystem stack. The most significant opportunities are the shared values created through the focus on innovation. This enables breaking barriers on knowledge and influencing with the open development community, engaging in an exciting way to address evolving challenges and opportunities combining MECs and SnapScale DLT.

### 7.2 XENIRO Economic Model

XENIRO refers to tokens as a cryptographic string of numbers relating back to data (used for specific functions in specific systems) that serve as an economic incentive within the ecosystem, providing access to the XENIRO platform. The tokens are a breakthrough in network design that enable the creation of an open, decentralized network that combines the best structural properties for open and proprietary networks. This is also a new way of incentivizing open network participants. Through enabling this network, tokens could reverse the centralization of the Internet of Everything, creating shared computing resources at the edge of the network, while keeping the control of these resources decentralized in MNOs infrastructure.
Token networks offer a common goal to all participants through the growth of the network that escalates to many service creations through development of decentralized applications. This could take on various forms through (A) Staking based on the SnapScale DPoS consensus algorithm, rewarding selected witnesses (MNOs) for securing the network and verifying transaction on their MEC infrastructure (B) Token based governance allows stakeholders on the XENIRO platform to vote for direction on the platform, whereby stakeholders can propose changes to the networking programming upgrades, features, partnerships on which token holders can vote with their holdings. By doing so, they become part of the governing process within the XENIRO platform. (C) Developers support the platform when they have ownership stake on it. The XENIRO network will distribute tokens to key stakeholders and contributors to incentivize them to develop and enhance the platform even further (D) With XENIRO based services, tokens will be needed by enterprises accessing the applications executed by the MEC, that could be for a specific transaction or require further MEC resources (bandwidth, compute, storage, networking).

The XENIRO economic model feeds the ecosystem through governance, provides incentives to developers, access to DApps at the edge, and network contribution are some of the drivers in utilizing these tokens within the framework.

The economic model built on the network effect is highly relevant in this context where the platform becomes a powerful enabler in generating value for MNOs. XENIRO platform is a strategy to mobilize and empower the whole DLT IoT ecosystem. To understand the XENIRO economic concept, one would apply the Metcalfe’s lawxxvi that has become an important formula for applying network effects.
The network effect (Figure 24) as explained by Metcalfe’s law states that: The value of the network is proportional to the square of the number of connected nodes. As the physical cost of the network grows linearly, its value increases exponentially. In other words, if we were to apply a locally connected MECs or even a federated globally connected MECs, via XENIRO platform, it becomes more valuable as they become connected. Let us illustrate this with an example: With Metcalfe’s Law, n refers to the number of nodes, each connection IoT makes is calculated as \( n(n-1)/2 \). Assuming on a global scale, there are 6.5xxvii million distributed radio base stations, assume each base station is assigned with a MEC, we have a rough estimate of 6.5M MECs.

GSMA has registered more than 750xxviii MNOs spanning across 220 countries. Let us assume 325,000 MECs worldwide (5%) are connected to the XENIRO platform, making an average of 433 MEC nodes per operator around the world (taking a very conservative number). If 325,000 MEC nodes are deployed in serving IoT devices, through applying the Metcalfe’s law, there will be almost 52.8 billion connections made. If half of 52.8 billion connections automates transactions (that is repetitive) on the XENIRO platform, one can imagine the immense monetization opportunities with XENIRO’s proposed architecture for all stakeholders in the ecosystem. If we extend the optimism and double this to 650,000 MEC nodes worldwide (10%), the IoT device connections will increase to over almost 211 billion, highlighting how the corresponding value can proliferate. As we double the MEC nodes deployed, the number of IoT device connections quadruples. There are also negative network effect dependencies, of which scalability is the most critical component. DLT business adoptions are unable to reach the full network effect potential today because a good majority of these DLT protocols are not configured to scale for modern day business applications, thus annihilating and even reversing the network effect.
In a connected world, MNOs infrastructure is what powers the modern-day society. As the industry migrates toward 5G evolution, this technology possesses the potential to reboot the next era of industrialization. Hyperconnected 5G world has just arrived, and we are on the brink of the next evolution in connectivity. The potentials are virtually unlimited, interconnecting a plethora network of smart machines & devices across industries. MEC, on the other hand, is a crucial building block for the vision of 5G networks. 5G and MECs create such a powerful combination that essentially becomes a new network on its own, connected through SnapScale DLT that we call “xGRID”. Services inspired by SnapScale DLT have the potential to disrupt in multidimensions. MECs will no longer be labeled as a cost center, but a profit center, acting as a bank in processing billions of IoT device transactions on the SnapScale DLT.

To address the trilemma principal, we summarized XENIRO’s proposed solutions, solving the key concerns in these following areas:

- **Scalability**: DPoS + DAG (hybrid SnapScale DLT) are some of the fastest processing algorithms in the industry today.
- **Security**: ORDOS ASIC chip is designed as an added fortified secure layer, that supports Privacy Encryption (ZKP) and boost performance levels for all IoT transactions on the SnapScale DLT.
- **Decentralization**: Distributed MEC architecture with compute, storage and networking resources at the edge, ensuring the xGRID network reach an optimal level of decentralization.

MECs will no longer be labelled as a cost center, but a profit center, acting like a bank, in processing billions of IoT device transactions on the SnapScale DLT.
Figure 25 summarizes XENIRO’s end-to-end portfolio in optimizing SnapScale DLT within the IoT domain. For DLTs to become full adoptable in a commercialized setting, we need to leverage (I) SnapScale algorithms in combination with the (II) XAP + MEC infrastructure and (III) ORDOS ASIC chip to be thoroughly optimized and fine-tuned for deployment. To achieve an enriched user experience with DApps, MNOs play a significant role within this framework, supported by the DLT developer community, to propagate decentralized IoT application adoption at the edge. Focusing on finetuning DLT algorithms alone, will “NOT” result in scalability breakthroughs within this thriving industry.

XENIRO’s full stack portfolio in combination with MNOs’ 5G assets is the transformative platform the industry has been seeking. MEC has created a significant amount of interest amongst the industry with major potentials. There are plenty of business opportunities MNOs could explore around DApp hosting at the edge. That could include X-as-a-Service model, leasing of decentralized resources, system integration, decentralized B2B2X solutions, providing DLT QoS and privacy encryption services, federated DApp roaming through NFV NS, and the list goes on! With these business models enabled by XENIRO’s solution stack, MNOs can opt for services that fit within their capabilities. This is the perfect opportunity for MNOs to revive lost territories, in counterstriking against the giant cloud providers, through their infrastructural assets, and start nurturing an innovative, open, distributed, decentralized edge ecosystem.

To build MNO alliance amongst partners in the 5G era will be a challenge. However, with the XENIRO’s xGRID network vision, alliance between MNOs may be accelerated through the connections
over the SnapScale DLT. Joint federated NS strategies amongst MNOs make it possible to extend MNOs business to multiple countries and broaden the market of potential customers. Where an IoT device in one country, can automate smart contract transactions with another through a decentralized and distributed network, that was inconceivable a few years ago. But possible now, with 5G + NFV + MEC + SnapScale DLT as the next emerging technologies.

Our aim is to foster innovation through flexible exposure of the MNOs network value creation capabilities featuring SnapScale DLT, that is set to bring Trust (Security, Identity and Privacy), Service (Device Interaction, Transaction, Performance, QoS), Experience (Real-time, Tactile, Customized), and Transformation (Monetization, New Ecosystem, Industry collaboration, Standardization) in this next wave of technology evolution.

With current trends, XENIRO continues to see breakthroughs in the design and development of DLT protocols. We will strive for openness that is accessible to every MNO player within the entire ecosystem. MNOs can start contributing to the XENIRO community and establish their influences, having their voices heard to ensure their capabilities are being implemented into the DLT protocol, thus, solidifying an ecosystem that will eventually benefit the whole community.

This will primarily take us one step closer to the vision of a fully interconnected world. We sincerely invite the MNO industry to join the XENIRO ecosystem in navigating new paths to disrupt, with the realization of 5G potential, or continue to face ever-growing accelerated disruptions.

“The Sky is the limit”
Acknowledgment


ii https://www.forbes.com/sites/jonathanponciano/2018/06/06/worlds-largest-telecom-companies-2018/#5d0ce06f7d39

iii IDC Forecasts (June 2018) https://www.idc.com/getdoc.jsp?containerId=prUS43994118

iv Business Insider 2018

v Gartner 2017 IoT Report

vi Ericsson Mobility report | IoT Forecast


x https://github.com/ethereum/wiki/wiki/Sharding-FAQs


xiv https://www.mobileworldlive.com/blog/blog-global-base-station-count-7m-or-4-times-higher/


xvi https://github.com/ethereum/wiki/wiki/Sharding-FAQs

Daniel Larimer, “Delegated Proof-of-Stake (DPOS),” 2014


https://en.wikipedia.org/wiki/Von_Neumann_architecture


https://z.cash/technology/zksnarks/

https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

https://en.wikipedia.org/wiki/Metcalfe%27s_law

https://www.mobileworldlive.com/blog/blog-global-base-station-count-7m-or-4-times-higher/

https://www.gsma.com/membership/who-are-our-gsma-members/full-membership/