# IoADT: Internet of Autonomous Decentralized Things Part - I

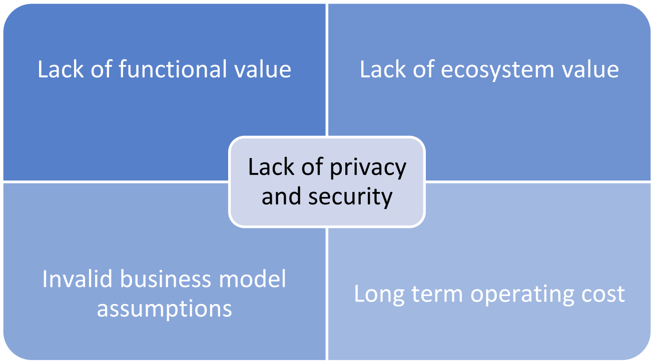
IoT architecture is continuing to flatten as more devices directly connect to networks and edge devices are becoming more intelligent. These devices are performing data aggregation, data integration and routing directly to other operational devices.

The rise of inexpensive general purpose computing has been accompanied by the availability of inexpensive sensors and actuators that today are cheap enough to embed in a device even if they are not used. Tremendous advances in cloud computing enable storage and analytics of the vast amounts of data generated by these sensors. Fueled by ubiquitous connectivity and the availability of billions of IP addresses with IPv6, the number of connected devices is forecasted to surpass 25 billion in 2020, up from 2.5 billion in 2009 and 10 billion today.

Looking forward, an increase in open web-service application program interfaces (APIs) will allow devices to connect and work smoothly as part of complex, multi-vendor networks. The result: a proliferation of hundreds of billions of devices that will be no more expensive than their dumb counterparts, yet able to operate and act as part of complex, integrated systems. As with prior revolutions, this one will usher in another order-of-magnitude reduction in cost.

So far, the first wave of the IoT has focused on very high-value applications. There have been visible successes in continuous monitoring of smart buildings, jet engines, automated smart meters and remote healthcare management. Market expectations and valuations, however, have been enormous – as much as 10 to 20 times revenue, even though revenues have been relatively small, particularly in the consumer space. This is largely a result of the cost and complexity of most IoT solutions, as well as enterprises and entrepreneurs treating the IoT as if it were just another computing platform, and applying the same set of business models: services, ecosystems, applications and analytics.

## Five big problems are holding back the development of a massively scalable internet of things:



### A lack of functional value

Many IoT solutions today suffer from a lack of meaningful value creation. The value proposition of many connected devices has been that they are connected – but simply enabling connectivity does not make a device smarter or better. Connectivity and intelligence are a means to a better product and experience, not an end.

### Lack of ecosystem value

Many smart device manufacturers have improbable expectations of ecosystem opportunities. While it makes interesting conversation for a smart TV to speak to the toaster, such solutions get cumbersome quickly and nobody has emerged successful in controlling and monetizing the entire IoT ecosystem. Ecosystem value is the whole greater than the sum of parts.

### Invalid business model assumptions

Most IoT business models also hinge on the use of analytics to sell user data or targeted advertising. These expectations are also unrealistic. Both advertising and marketing data are affected by the unique quality of markets in information: the marginal cost of additional capacity (advertising) or incremental supply (user data) is zero.

### Lack of privacy and security

The Internet was originally built on trust. In the post-Snowden era, it is evident that trust in the Internet is over. The notion of IoT solutions built as centralized systems with trusted partners is now something of a fantasy. Most solutions today provide the ability for centralized authorities, whether governments, manufacturers or service providers to gain unauthorized access to and control devices by collecting and analyzing user data. For widespread adoption of the ever-expanding IoT, however, privacy and anonymity must be integrated into its design by giving users control of their own privacy

### Long term operating cost

Many existing IoT solutions are expensive because of the high infrastructure and maintenance costs associated with centralized clouds and large server farms, in addition to the service costs of middlemen. There is also a mismatch in supplier and customer expectations. Historically, costs and revenues in the IT industry have been nicely aligned. With the IoT, it is unlikely that there will be enough margin for companies to cover several years of support and maintenance. The cost of supporting and serving billions of smart devices will be substantial – even something as simple as maintaining centralized servers that distribute regular software updates

In light of economics, what is the business model that is going to be sustainable and then supported by resilient underlying architecture and platform? Let's switch gears and expand our aperture a little bit. When you look at the business we are looking at and the challenges I described above in terms of functional value, ecosystem value, invalid business case, privacy & security and long term operating cost. We are dealing with a wide spectrums of things ranging from smart phones, laptops, cars, house, building and subways. These things are going to be around for quite some time. What's going to be the operating cost of maintaining these things? This is a very profound problem and needs to be addressed.

There are three things that are very important that we need to do to save the future of Internet of things

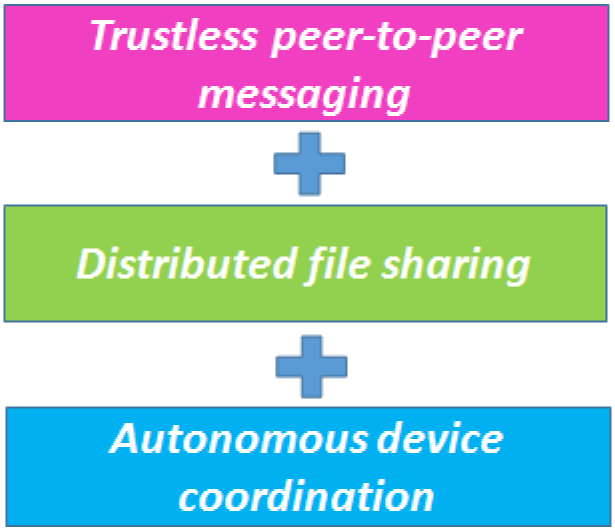
1. Build better products that address the functional challenge
2. Create sustainable and endurable business models
3. Create underlying resilient decentralized highly efficient platform

So how do we address the scale and security issues that are intrinsical? How do we bring order, trust, privacy and yet at the same time not have a command and control model because intrinsically that's what a peer-peer model is where trust and capability has to be built into the foundation of P2P model. What is needed to grow to the scale of billions of billions of devices?

As the IoT scales exponentially, decentralized networks have the potential to reduce infrastructure and maintenance costs to manufacturers. Decentralization also promises increased robustness by removing single points of failure that could exist in traditional centralized networks. By shifting the power in the network from the center to the edges, devices gain greater autonomy and can become points of transaction and economic value creation for owners and users.

## Three foundational functions of Autonomous Decentralized Things

To perform the functions of traditional IoT solutions without a centralized broker, any decentralized approach must support three foundational functions:


Trustless peer-to-peer messaging
Distributed file sharing
Autonomous device coordination

### *Trustless peer-to-peer messaging*

The decentralized nature of peer-to-peer (P2P) networks increases robustness because it removes the single point of failure that can be inherent in a client-server based system. As more nodes are added and demand on the system increases, the total capacity of the system also increases, and the likelihood of failure decreases. If one peer on the network fails to function properly, the whole network is not compromised. In contrast, in a typical client–server architecture, clients share only their demands with the system, but not their resources.

A P2P distributed architecture enables participants of the network to be equally privileged. Peers can share resources without dependency on a central cloud or server thereby optimizing resource utilization and cost involved in subscribing to a central service. Introducing peers with diverse capabilities and resources could further strengthen the overall stability and performance of the system without dependency on external 'controlling' or 'mediating' entities.

### *Distributed file sharing*

In the P2P messaging approach, there is no centralized broker of messages or controller of data. The key characteristics of this approach are

1. Trustless, encrypted messaging and transport
2. Low latency with guaranteed delivery
3. Store and forwarding of messages with hop-on to other connected devices.

Such messaging capabilities can be achieved using structured P2P networks where the overlay is organized into a specific topology and the protocol ensures that any node can efficiently search the network for another peer. The Distributed Hash Table (DHT) can be used to implement such networks, enabling peers to search for other peers on the network using a hash table with (key,value) pairs stored in the DHT. Each end point would generate its own unique public-key based address (a hashname) to send and receive encrypted packets with other end points and any participating node can efficiently retrieve the value associated with a given key.

Distributed file sharing enables decentralized software/firmware updates, device based analytics reporting and secure file and data sharing, sometimes of large orders of magnitude. Such transfers can also be achieved by means of distributed P2P networks using DHT - Bit Torrent being a famous example of a distributed P2P protocol that enables file sharing.

## *Autonomous device coordination*

Apart from P2P messaging and distributed file sharing, the third foundational function required in a decentralized IOT solution would be some form of autonomous device coordination. In the absence of a single arbiter of roles and permissions, such a solution grants greater power to the owners of devices to define how devices interact via rules of engagement.

A key difference in this approach is that this recognizes that different devices, by virtue of operating within specific constraints imposed by physical or business proximity and interoperability, could have varying levels of trust between themselves. This becomes possible as devices change from mere end points orchestrated by a controller to peers on a decentralized network. Achieving this would be central to the vision of an IoT world where devices and products can engage in autonomous transactions and form trustless networks.

By not requiring a third-party arbiter of roles and permissions, an autonomous device coordination approach empowers owners of devices to define and manage their own interactions. Simple device coordination functions include registration and authentication. More complex interactions require the owner or user to define rules of engagement. These rules could be proximity-based (physical, social or temporal), consensus-based (selection, validation or blacklisting), or triggered by other device stimuli.

Another form of device coordination is contracts – simple agreements about actions or control, more complex financial contracts involving payments or barter contracts that allow devices to exchange their resources for a service. Digital checklists allow devices to maintain themselves to prevent failure.

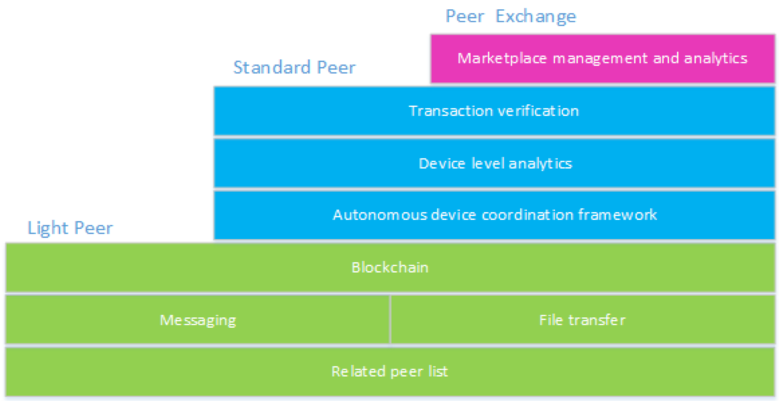
## Building a blockchain-based IOT

The current emerging paradigm for this decade could be the connected world of computing relying on blockchain cryptography. The connected world could usefully include blockchain technology as the economic overlay to what is increasingly becoming a seamlessly connected world of multi-device computing that includes wearable computing, Internet-of-Things (IoT) sensors, smartphones, tablets, laptops, quantified self-tracking devices (i.e., Fitbit), smart home, smart car, and smart city. The economy that the blockchain enables is not merely the movement of money, however; it is the transfer of information and the effective allocation of resources that money has enabled in the human- and corporate-scale economy.

Blockchain technology’ s decentralized model of trustless peer-to-peer transactions means, at its most basic level, intermediary-free transactions. However, the potential shift to decentralized trustless transactions on a large-scale global basis for every sort of interaction and transaction (human-to-human, human-to-machine, machine-to-machine) could imply a dramatically different structure and operation of society in ways that cannot yet be foreseen but where current established power relationships and hierarchies could easily lose their utility.

Blockchain foundation is the underlying technology under the IoADT ecosystem. The notion here is you look at assets around which you can wrap transactions and it’s a highly decentralized, highly autonomous serial database ledger where transactions gets logged, with tremendous intrinsically built-in contract enforcement as long as most of the nodes are honest. It ensures trust, based on longest chain in the blockchain even if there are renegades. Those renegades are put aside because it’s the longest chain that wins and when there are more honest nodes the longest chain is going to be hard to outpace. The blockchain technology provides intrinsic trust in the peer-to-peer apparatus as opposed to having a centralized party. There is no single point of failure and there is no need to trust all the participants.

## IoADT PEER Architecture



Foundational concept for IoADT is derived from an open source project being run by IBM know as ADEPT- that recognized the appropriate technology capabilities of different devices and would still meet the principle of decentralized autonomous P2P devices. ADEPT defines three broad categories of devices, described as Light Peers, Standard Peers and Peer exchange

**Light Peer**: The light peers are devices with low memory and storage capabilities. I expect these to be found in small sensors and devices supporting light applications. In the current day, I could think of a Raspberry Pi, a Beaglebone or an Arduino board as representative of the light peer. I assume the light peers would have no capability of storing blockchains, and would only retain its own blockchain address and balance inside the device in what is described as a "light wallet". For obtaining transactions in the blockchain pertaining to itself, the light peer would turn to another trusted peer

**Standard Peer**: In the next few years, I expect the processing power and storage capabilities of most products to increase as the cost of manufacturing high performing semiconductor chips declines. The additional cost to the manufacturer or the end consumer by designing products to have such hardware would be very small. So the washer of the future or the refrigerator would be equipped with higher storage and processing capabilities that makes it possible for these products to meet blockchain requirements, for a specified period of time, of not only themselves but also of the light peers in its trusted environment. I expect such products to become the standard or the norm in the years to come.
A standard device, at the core protocol level is very similar to a light device, but it would retain a part of the blockchain based on its capabilities. This could be its own recent transactions, but could also be for other lighter devices in the ecosystem that it has come to a contractual agreement with. A standard device would also be able to support a lighter peer in performing file transfers. It would have capabilities to store and forward messages to peers and perform light analytics for itself and other peers. The analytics capabilities are explored in greater detail later in this paper.

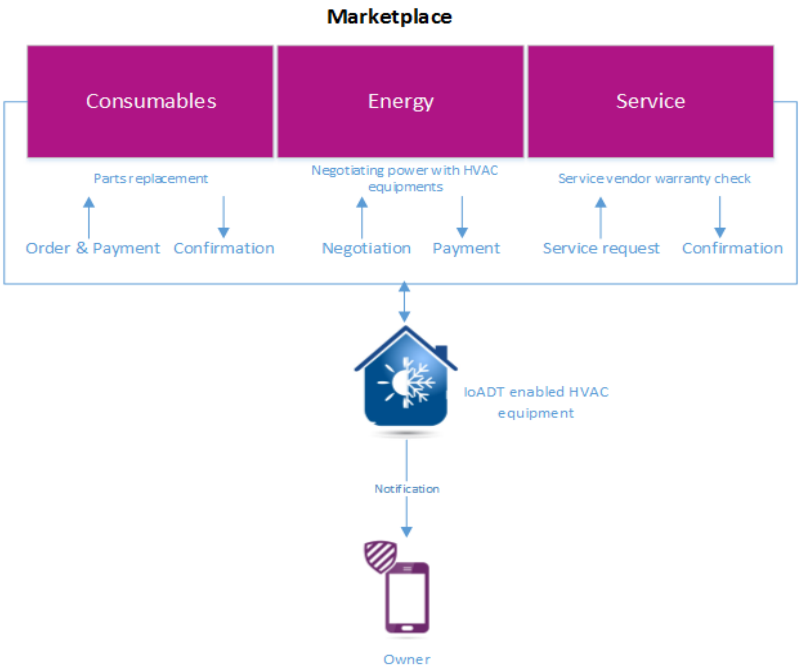
**Peer Exchange**: Peer exchanges are high end devices with vast compute and storage capabilities. They would be ADEPT peers, owned and operated by organizations or commercial entities and would be capable of hosting marketplaces. A marketplace would potentially require payment exchanges, analytical solutions, fraud detection, trade and legal compliance packages, demand supply matching solutions etc. Peer exchanges are also potential repositories for a complete copy of the blockchain and would provide blockchain analytical services.

Peer exchanges are also potential repositories for a complete copy of the blockchain and provide blockchain analytical services. The size of blockchains can rapidly increase in scenarios where a city or community may have millions of IoT devices. Even standard peers with advanced processors and storage may not be able to hold blockchain information for themselves and the peers they service for more than a few days. However, with the blockchain being the trusted source of information holding all product transactions, it is important to be able to access it at a regional or community level going back in time, in some cases back to the start of a product's life.

## Transforming the IoT into Internet of Autonomous Decentralized Things

By enabling devices to engage autonomously in a decentralized ecosystem and supporting complex marketplace transactions, the IoT is expected to improve the utilization and profitability of physical assets and devices. By transforming every device into a point of transaction and economic value creation for owners and users, the IoT will create new real time digital economies and new sources of value.

A simple B2C use case of how an Autonomous Decentralized Thing in context to a building could be a HVAC equipment capable of performing self-service and maintenance and even negotiating with other devices – both in the home and outside to optimize energy consumption and all that without a central controller orchestrating or mediating between devices.



Autonomous Decentralized Things shows a great promise for tomorrows IOT. As economy of autonomous decentralized devices. Thanks for major advances in both technology and software it is not possible to bring transaction processing, marketplaces and intelligence to virtually every device, anywhere.

Distributed systems like IBM ADAPT and Filament can make businesses and consumers more efficient and open a huge of economic opportunities. In the next part of this thought paper I will drill deeper into the technical stack for IoADT and will peel apart and peel back the architecture edition being implemented by IBM and Filament.

## References

1. https://filament.com/assets/downloads/Filament%20Foundations.pdf
2. http://www.the-blockchain.com/docs/Blockchain%20as%20a%20P2P%20protocol%20for%20the%20Internet%20of%20Things.pdf
3. http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/
4. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03620USEN&attachment=GBE03620USEN.PDF%E2%80%9D