ADEPT: An IoT Practitioner Perspective

DRAFT COPY FOR ADVANCE REVIEW

Final copy to be distributed through IBM Institute for Business Value.
Visit ibm.biz/devicedemocracy

I. Device Democracy: Approach & Vision

The 2014 IBM Institute for Business Value paper "Device Democracy: Saving the future of the Internet of Things" (ibm.biz/devicedemocracy) makes the case that centralized approaches to building an internet of hundreds of billions of things are expensive, lack privacy and are not designed for business model endurance[i]. In addition to business challenges associated with scale and complexity of the IoT, there are technical challenges to be explored. What challenges exist in the widely practiced centralized IoT model and what alternative approaches are worth pursuing?

Our ADEPT platform – Autonomous Decentralized Peer-To-Peer Telemetry is an effort to prove the foundational concepts around a decentralized approach, one that will offer greater scalability and security for the IoT.

The purpose of this white paper is to outline the key objectives in the development of this platform, the challenges to scaling this technology, and a roadmap for how the architecture should evolve in the future. The paper is intended as a starting point for collaborative discussion both internal to IBM and externally with open source communities working on similar problems.

II. Key Objectives for Proof of Concept

In building a proof of concept for a decentralized IoT, we wanted to establish a foundation on which to build and to prove several key capabilities. These include:

1. Distributed Transaction Processing & Applications: Accomplish foundational IoT process tasks without the need for any centralized control infrastructure. Though many commercial systems in the future will exist as hybrid centralized-decentralized models, we wanted to start with a fully distributed proof.

2. Robust Security: We wanted to implement multiple layers of security and encryption in transaction processing, storage, and transport. We also wanted to design an architecture that can withstand individual points of failure and operate in a model where no trusted third party is required to secure transactions. Furthermore, we believe that transparency is now the foundation of security and so any work in this area must be done as open source.

3. Privacy By Design & Default: Our vision is that privacy is a key feature of future systems and that users should have to take specific action to reveal their identities. Most existing systems require users to take action to enable privacy, we believe in the opposite approach.

4. Designed for Commerce & Marketplaces: Finally, we believe the IoT will create an Economy of Things. Every device, every system can be a point of transaction and economic value creation for owners and users. Every device should be able to engage in multiple markets, both financial and non-financial and should be able to autonomously react to changes in markets. These capabilities will be crucial to everything from the sharing economy to energy efficiency and distributed storage.

While not every one of these principles is fully developed in our proof of concept, we believe the architecture we have developed reflects those goals and is capable of implementation as we expand the capability of our solution.

III. Key Solution Components

Peer-to-peer decentralized networks

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.

There has been much interest in emerging P2P networks because they provide a good substrate for creating large-scale data sharing, content distribution and application-level multicast applications. These P2P networks try to provide a long list of features such as: selection of nearby peers, redundant storage, efficient search/location of data items, data permanence or guarantees, hierarchical naming, trust and authentication, and anonymity. [ii]

P2P messaging and distributed file transfers

In the P2P messaging approach, there is no centralized broker of messages or controller of data. The key characteristics of this approach are a) trustless, encrypted messaging and transport b) low latency with guaranteed delivery and c) 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 [iii] 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 our vision of an IoT world where our devices and products can engage in autonomous transactions and form trustless networks.

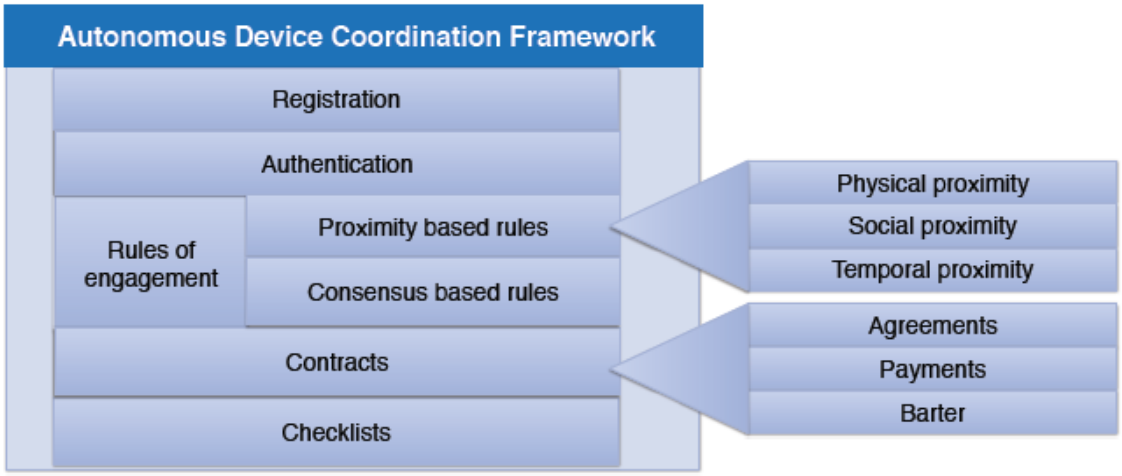
In order to achieve this, we would require a mechanism to equip the devices and products to enter into contractual agreements with other devices. These contracts would define the way they transact – whether they be simple agreements of actions or control, financial agreements involving payments or loans or to simply enable devices to barter their resources in exchange for some service.

Another important aspect to consider is security. In addition to the security offered by the protocols, the operational security in transactions needs to be considered. In this world of a largely P2P network of interacting devices that often function autonomously and where the parties are untrusted and may even be malicious, how can networks secure themselves? Our P2P networks would need to self-organize and achieve consensus based coordination to guard against routing or denial of service attacks. And if there are players in the network that are acting in a manner contrary to the “rules of engagement” – say

a manufacturer violating opt-in policies or a service provider introducing corrupt firmware updates or even a malicious/hacked device – consensus would be critical to quarantine and protect the network of devices.

In order to achieve the autonomous device coordination we explained earlier, it is important to consider user experience. In the ADEPT world users or the device owners are granted the power to set up and decide rules of engagement for their devices. To achieve this in an efficient manner, there is the need for a device coordination framework that defines roles and enables appropriate behavior of devices for an autonomously functioning IoT. Such a device coordination framework would primarily serve three types of actors – the users/owners of devices, the devices and the manufacturers.

From a user's perspective, the framework would enable creation and maintenance of rules of engagement of their devices and creation of digital checklists to prevent failure.



The devices would be able to autonomously authenticate peers and self-maintain.

The manufacturers would be able to use the framework to register devices in a universal asset registry enabling them to track device information and specifications over its lifetime and transfer maintenance responsibility to devices and third parties. The framework would be the key to enable a simple and reliable way of setting up and using devices with the ADEPT architecture stack.

To implement these contract-based device interactions and to achieve consensus based device coordination across a global network of devices, the blockchain technology platform was chosen.

IV: Integrating the Components into an Architecture

Blockchain and Device Specific Architecture

The blockchain is a long ledger of transactions shared by participants of the network. A full copy of the blockchain will have a record of every transaction ever completed in the network. Every participant in the blockchain can maintain its own copy of this ledger of transactions, though ideally, the amount of data stored would vary based on capability, need and preference. Every block contains a hash of the previous block. This enables the blocks be traced back even to the first, the genesis block. It is computationally prohibitively difficult and impractical to modify a block once it is created, especially as the chain of subsequent blocks get generated. Blocks in shorter chains are automatically invalidated by virtue of there being a longer chain – all participants adopt the longest chain available.

Blocks are generated by a computation-intensive process called mining. Mining allows nodes to reach a secure, tamper-resistant consensus. Mining is also the mechanism used to introduce new coins or tokens of transaction into the system: Miners are paid any transaction fees as well as new tokens, based on the specific implementation model. There are various mining algorithms, primarily based on Proof of Stake or Proof of Work approaches. The cryptocurrency space is actively engaged in investigations on optimizing different aspects of the technology including addressing challenges like scalability.

It is important to note that while BitCoin contains an escalating difficulty in the mining process to restrict the issuance of currency, no such restriction is necessary in our vision of the world. We need sufficient Proof of Stake and Proof of Work to ensure network integrity and cryptographic security but without the need to impose an arbitrarily increasing computation cost and carbon footprint on the process.

Blockchains for the IoT

Applying the blockchain concept to the world of IoT offers fascinating possibilities. Right from the time a product completes final assembly, it can be registered by the manufacturer into a universal blockchain representing its beginning of life. Once sold, a dealer or end customer can register it to a regional blockchain (a community, city or a state).

Once registered, the product remains a unique entity within the blockchain throughout its life. So in a blockchain based IoT, the possibility of maintaining product information, its history, product revisions, warranty details and end of life in the blockchain means the blockchain itself can become the trusted product database. Take an example: Imagine a world where a smart washer is able to detect a component failing, can check from the blockchain if the component is in warranty, place a service order with a contracted service provider, and the

service provider can independently verify the warranty claim – again from the blockchain – and all this, autonomously. In such a world, we would redesign and simplify the way we design our master data management systems, after sales systems and order processing and management. The blockchain based decentralized IoT can become a truly revolutionary approach to transaction processing among devices.

Device capabilities and the nature of trust

Different devices are built differently to perform specific functions. The capabilities of these devices also vary widely by computing power, networking capability, storage space, power supply, whether they are stationary or mobile, to mention a few. It does not make sense for all devices to store the entire or even a huge portion of the blockchain. It is often unnecessary and impossible for some of the smaller devices, say a Raspberry Pi or a Beaglebone to do so.

The nature of trust in such an autonomous model could be an evolving one. These devices would be part of ecosystems that enable and at times require different levels of trust. As more and more transactions occur between peers, trust could evolve between them, thereby meaning what once started as interactions between two trustless peers can over time become a semi-trusted or even a trusted relationship.

There could also be instances where the low life span of the device or relative insignificance of its role in a specific transaction means that blockchain based peer verified transactions aren't necessary. So the trust and extent of verification required depends on many factors: the type of device, the nature of the interaction, the kind of relationship between the devices and also the constraints imposed by the owners of the device on what the devices can and cannot do in specific circumstances.

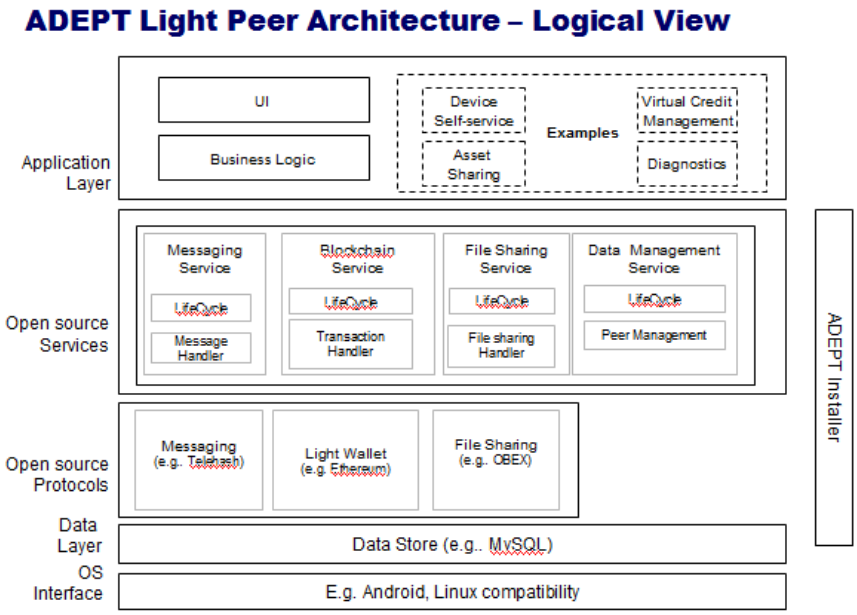
Taking all of the above into consideration, we took an architecture approach – christened ADEPT (Autonomous DEcentralized Peer to Peer Telemetry) - that recognized the appropriate technology capabilities of different devices and would still meet the principle of decentralized autonomous P2P devices. We looked at three broad categories of devices, described as Light Peers, Standard Peers and Peer Exchanges and defined the architecture stack that would apply each of these categories.

ADEPT Peer Architecture

Our architectural approach has evolved from an original viewpoint that all points in the network are equal towards one that recognizes some level of differentiation. In particular, we recognize that many tiny devices may not have the full computational power and memory to manage the complete block-chain while

others may be powerful centers of commerce and interaction. Accordingly, our current architectural model has three levels of capability.

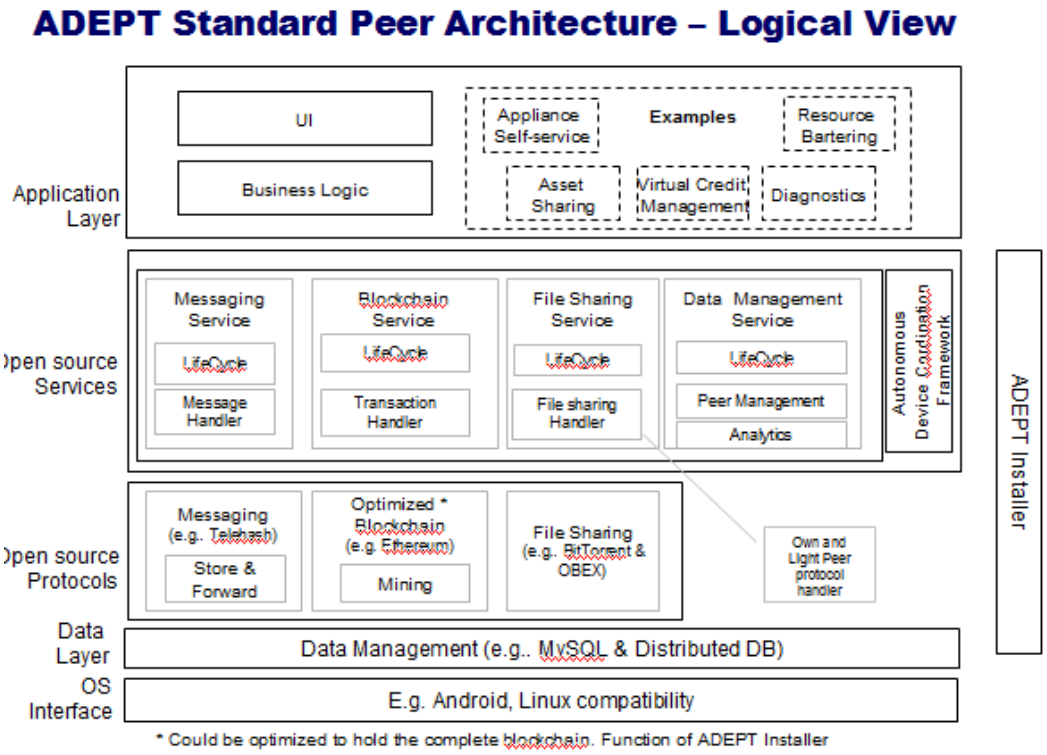
Light Peer: The light peers are devices with low memory and storage capabilities. We expect these to be found in small sensors and devices supporting light applications. In the current day, we could think of a Raspberry Pi, a Beaglebone or an Arduino board as representative of the light peer. We assume 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. The reference architecture we have envisaged for a light peer is shown below:



A light peer will perform messaging, retain a 'light wallet' with its addresses and balances and will perform minimal file sharing - for example, receive firmware updates or send summary of certain transactions to another peer based on a business or functional need. The file sharing mechanism for a light peer may not be BitTorrent which can become too heavy for it to support. It is expected to be closer to protocols used by today's mobile devices like OBEX.

Standard Peer: In the next few years, we 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. We expect such products to become the standard or the norm in the years to come.

So in our ADEPT architecture, the standard peers can hold blockchain information for a certain period of time. The reference architecture of the standard peer is as shown below:



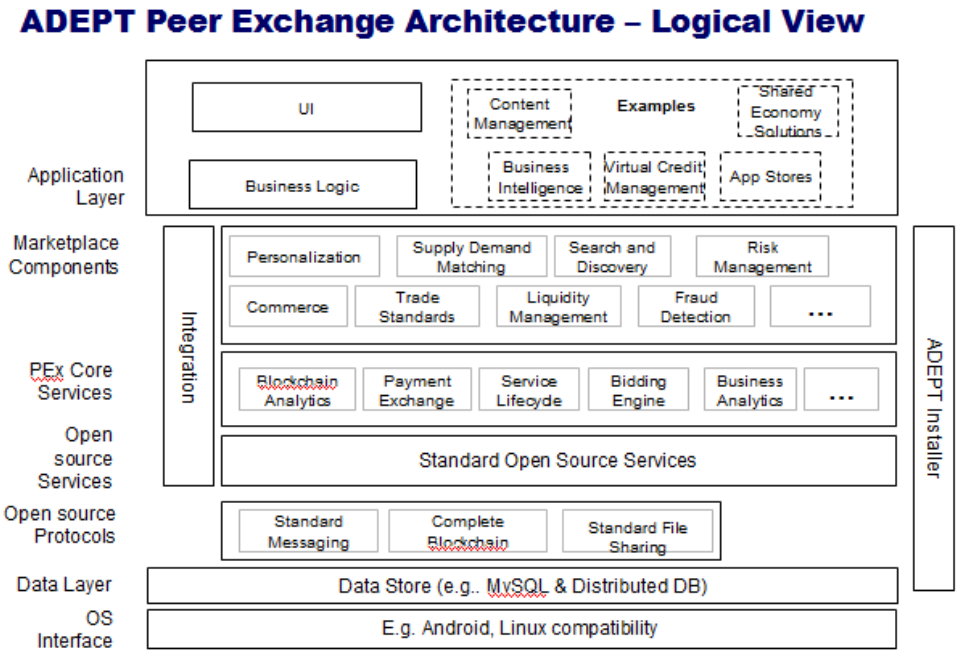
A standard device, at the core protocol level is very similar to a light device, but it would retain a part of the blockchain based on its capabilities. This could be its own recent transactions, but could also be for other lighter devices in the ecosystem that it has come to a contractual agreement 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.

The size of blockchains can rapidly increase in a world where every city or community may have millions or hundreds of 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 pertaining to 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 from the start of product life. For example a solar micro-grid may have been commissioned a decade ago or the smart street lights may have been registered a few years back. For servicing or support, the blockchain may need to be accessed to verify the first registration or to know the installation details. We then have the need for peers with large processing and storage capabilities that can store the complete blockchain and do complex queries and blockchain analytics. The peer exchanges serve this function. We also foresee the peer exchange fulfilling the role of a demand and supply balancer between services demanded and offered by various assets and products across communities, somewhat akin to the role performed by current day financial exchanges. So resources offered by a set of assets in one community might turn to a peer exchange to find buyers in another. The peer exchange then becomes more than a large server or a cloud offering memory and technical support, it becomes the lifeline for new economic activities – the new silk routes – making possible the 'liquification of assets' argument set forth in the Device Democracy paper[iv]

The reference architecture for a peer exchange is shown below:



A peer exchange builds on the open source services core stack of a standard peer. The peer exchange will be able to offer commercial business solutions in the new decentralized IoT world. It would have core services that enable features like Blockchain analytics and running payment exchanges. It would also have marketplace components – building blocks of a marketplace on which large

business solutions could run. The peer exchange would also have the integration capabilities required to support and interoperate with other solutions.

Peer Lists

As devices become peers of a decentralized network, it is essential that every device is able to identify itself uniquely to peers in a verifiable manner, be able to retain details on its relationship with different peers and be able to identify the peer unambiguously across protocols. In order to do so, all ADEPT devices would have a peer list. This peer list will be synced with the coordination framework entries and be retained within each device with the adequate level of security.

Adopting ADEPT

In all the three reference architecture diagrams shown above there is a component called the ADEPT installer, that we see as playing an important role in devices being able to adopt the ADEPT stack. Our design integrates technology concepts from today's open source world that we see as promising and appropriate to decentralized P2P IoT. Any device could become ADEPT compatible if it meets the minimum prerequisites of network, processing and storage. The ADEPT installer would gauge the capability of the underlying device and be able to judge the right stack, extend of blockchain and data storage, analytics capability etc, and accordingly install the optimal stack on device.

V. Network Services

Data Management and Analytics

Data security and privacy is a major concern in centralized models. Decentralized IoT solutions should be able to manage data across devices for each ecosystem. Sharing data outside of the ecosystem should be based on rules defined by the owner of the ecosystem. Insights that can be gleaned by performing analytics on this data would also be managed within the boundaries of each ecosystem. In the ADEPT model, manufacturers would be able to enable devices to gather data but it would be the owners' decision whether to share the data. There would be a two-step authentication in place to ensure that unauthorized access to data is not easy. A distributed peer to peer database with distributed analytics capabilities therefore becomes an essential part of the ADEPT IoT solution.

VI: Foundational Components for Proof of Concept

We selected the following open source protocols to implement an ADEPT proof of concept (PoC): Telehash, BitTorrent and Ethereum,. We are grateful for the exceptional support we have received from these communities.

1. TeleHash: Of the many messaging protocols we considered, TeleHash seemed the most promising in approach and ideological match to our decentralized approach on IoT based on its Kademlia protocol based Distributed Hash Table implementation.
2. BitTorrent: BitTorrent utilizes bandwidth efficiently while discouraging leeching. We envision Torrent file sharing solutions being a critical part of the ADEPT architecture.
3. Ethereum: Ethereum's improvements to the traditional blockchain approach of Bitcoin and the Turing complete scripting languages they introduced were extremely compelling. The ability to create binding contracts and potentially Decentralized Autonomous Organizations led us to pick Ethereum as our PoC's blockchain technology.

VII. Use cases

The ADEPT PoC use cases initially identified spanned a spectrum of products with different capabilities. We identified three use cases - a very light device like a door lock, a mobile light device (wearable) and a standard, always connected device (a washer).

Samsung Electronics, a leader in the Mobile, Electronics and IoT space, collaborated closely with us on the development and demonstration of use cases, both B2B and B2C.

B2C Use Cases

IBM's B2C ADEPT use cases are centered on a washer, a common household appliance. We demonstrate how, using ADEPT, a humble washer can become a semi-autonomous device capable of managing its own consumables supply, perform self-service and maintenance, and even negotiate with other peer devices both in the home and outside to optimize its environment. We also have envisioned scenarios where micro-commerce solutions can be built using a set of ordinary home appliances. All this is achieved without a central controller orchestrating or mediating between these devices. This is what makes ADEPT truly revolutionary.

Use case 1: Reorder consumables

Most modern washers have analytics capabilities. We worked with the Samsung washer W9000 that has a detergent dispenser and can detect when supply runs low. In our ADEPT use case, the washer, in addition to detecting the detergent supply running low, is also able to:

- By querying its own peer list, determine that there is a pre-existing contract with a retailer for the supply of detergents
- Request a reorder of detergent through messaging
- Invoke the contract and make a trusted payment for the order
- Intimate the owner that a replenishment order is being placed

The retailer is able to, through his tablet,

- Determine the validity of the contract with the washer
- Receive the payment through the contract
- Generate the replenishment order
- Communicate to the washer, through direct messaging of the delivery details

Once the order was confirmed, the owner receives a confirmation message from the washer with delivery details on his phone.

Use case 2: Device self-service

Every device in ADEPT will have its key information such as device id, warranty information registered to the blockchain. It also stores its own warranty information in its local peer list. The washer, in this use case:

- Has its own inbuilt analytics to assess part or component performance. An impending part or component failure will trigger a service request.
- To ascertain warranty status the washer runs a check in its own local warranty details.
- To identify an appropriate service vendor, it then checks for peer rated consensus available over the blockchain
- Once a service vendor is selected, it raises a service request to the service vendor. If the appliance is in warranty, no payments are needed. If out of warranty, the appliance, the owner and the service vendor can enter into a contract to make a payment
- The service vendor upon receiving the request checks the warranty status of the device in the blockchain
- Upon verification, the service request is then accepted as a service order in the vendor's service system and the details directly sent back to washer with a notification to appliance owner.
- The owner and vendor can negotiate through messaging to modify the time at which the service professional will arrive to replace the part.

Use case 3: Power bartering

Physical assets are often unused a majority of the time. These underused resources cannot often be effectively utilized due to challenges around discoverability, trust, security and an effective payment mechanism. ADEPT proposes to address this in a big way. A small instance of this concept is captured in the power bartering use case.

The washer, in this use case,

- Is in a contractual agreement with other medium- to high- power consumers in the house.
- It subscribes to analytics from a feeder that indicates an upcoming spike in power price. Accordingly it determines that a power negotiation is required with its peers to ensure that the owner is not hit with punitive charges
- The washer, which is currently operational, detects that the TV is currently operational. It requests a power down from the TV.
- However, the TV's analytics indicate that it cannot power down, as this is peak TV viewing time
- The TV declines and in turn compensates the washer with owner approved tokens as per the contract conditions.
- The washer accepts the payment and delays its cycle by a couple of hours.
- The TV informs the viewers that an impending power price hike has been offset by the washer delaying its cycle.
- A second part of the use case has the washer negotiating directly with a community owned micro-grid. In exchange for specific KWH of power for one week, the washer offers a specific number of free wash cycles to community members at a later date, as per the contract set up by the owner with the community.

B2B Use Case

AdCast

The ADCast Solution owner has multiple large format displays (LFDs) hosted at strategic locations. The owner will lease out display space on the devices to candidates after reviewing their content. The availability of display slots is published by the ADCast owner. Candidates can access this information, submit the request for slots and upload the content through ADEPT's file sharing technology. Once the content is approved, it is automatically transmitted to all approved devices to be displayed at appropriate time slots. Payment for the service is done through the cryptocurrency feature of ADCast.

VIII. Key Challenges for Scaling

There are an enormous number of challenges that must be addressed to scale up this approach to billions of devices. Many of these challenges are being addressed by the rapidly growing developer communities. We have categorized our major challenges into three areas:

Messaging:

TeleHash and similar distributed Hash Table based messaging protocols are quite promising as potential messaging technologies for tomorrow's decentralized peer to peer Internet of Things. Still, there are challenges yet to be addressed:

- Guaranteed message delivery over a UDP based protocol is a challenge.
- Concepts of store and forward are presently under consideration. This kind of feature implementation would be a critical requirement for a decentralized network of semi-autonomous peers in order for messages to reach the intended recipient even when said recipient is not at present connected to the network.
- Ability to create arbitrary groups for communication, gracefully disbanding such groups would be a good feature to have. Creating consensus across the spectrum of devices through communication is also an interesting challenge.
- The messages are structured in JSON format today. As the number of devices and their transactions increase, the size of the message could be a challenge. This could be addressed through implementations like JSONH.
- Smooth message traversal across multiple networking protocols like WiFi, Bluetooth, BTLE, 6LoWPAN, Zigbee among others will also be a necessity for wide adoption of each of these technologies by themselves and the ADEPT stack as a whole.
- Integrating the messaging layer with the blockchain layer, not only for interoperability, but also to perhaps capture some critical 'trusted' communications for future verification, potential monetization or posterity are interesting points of investigation for an ADEPT IoT solution.

File Sharing:

Primary research around peer to peer file sharing has been focused around performance challenges, problems like free riding etc.

- When multiple clients are behind different NAT systems, there have instances of challenges in effective communication.
- Though Torrent is the most stable of peer to peer file sharing protocols, it may not be appropriate for light devices in the decentralized peer to peer IoT solution.

Blockchain:

- Perhaps the biggest challenge faced by all cryptocurrencies today is scalability. Multiple efforts (like sidechains, treechains and mini-blockchains) are ongoing to address this problem. While each approach has its merits and demerits we are yet to see consensus on a common approach across the board. A blockchain to cater to hundreds of billions of devices needs to be scalable.
- In ADEPT, we also have a concept of universal versus regional blockchains, which could be realized through a potential combination of some of these novel approaches. We are closely following the developments in the open source space to help address this requirement.
- Anonymity is also a contentious point in the cryptocurrency space. While bitcoin is generally considered sufficiently anonymous, there are proven instances where owners of specific bitcoin wallets were identified by IP address. As ADEPT goes more mainstream, we will have much better clarity of the level of anonymity an ADEPT transaction would require.
- There could also be multiple anonymity levels based on the nature of a transaction or the preference of the initiator or participants of a transaction. It would therefore be advantageous to closely study anonymity efforts like Dark Wallet and understand better how core concepts like built-in trustless mixing might be leveraged if needed.
- Ethereum is still in beta and evolving rapidly. There are some challenges, like the unavailability of a light wallet, for instance, that are being addressed in the core technology in time for release in 2015.
- When considering blockchain implementations, there are also challenges to porting what is essentially a cryptocurrency to an Internet of Things asset and transaction ledger. What makes perfect sense in a core crypto-currency may need to be altered to better fit an IoT environment.

IX. Next Steps for Architecture Strategy

ADEPT is the promise of tomorrow's Internet of Things. We have successfully completed a PoC of ADEPT. However, in order for ADEPT to develop further and become a commercial success, it is imperative that the core technologies be made more robust to meet the challenges that a peer to peer network of hundreds of billions of devices will impose on the system. We propose to explore the developments in the core technologies further. Through collaboration and an effective partnership between the IBM ADEPT team, Samsung Electronics (as a key collaborator and joint research partner) and the open source community, the ADEPT solution could be made robust, truly decentralized and scalable to meet the needs of not just hundreds, but thousands of billions of IoT peers, providing a low cost, scalable, long-lived and evolving IoT solution.

X. Contributing & Leveraging

As a first step in this collaboration effort, we will be sharing the code developed as part of the ADEPT PoC effort. An API suite development effort is ongoing for the ADEPT core stack. All these work products are to be made available at a later date on IBM BlueMix and Git.

XI. Conclusions

As we wrote in Device Democracy paper, the humble work of transaction processing is the foundation of modern computing workload. Thanks to major advances in both device technology and software, it is now possible to bring transaction processing, marketplaces, and intelligence to every device everywhere.

We believe that distributed systems like ADEPT will make our planet smarter, more efficient, and open up a huge range of economic opportunities. We believe these technological changes represent the biggest revolution since the origin of general purpose computing and transaction processing systems.

Revolutions, however, are not for the faint of heart. To move ahead, we must leave behind the certainty and comfort that comes with dealing with well-proven technologies. There are significant scalability challenges associated with distributed systems, not to mention issues with security, coordination, intellectual property management, identity and privacy. Many of the smartest people are working on these challenges and contributing to the open source foundation for these technologies.

There is one strategy, however, that offers certainty: sitting on the sidelines and waiting for others to pioneer this technology: when the risks have been resolved it will be far too late to catch up with the market leaders.

[i] Device Democracy: Saving the future of the Internet of Things. ibm.biz/devicedemocracy
[ii] Survey and comparison of peer-to-peer overlay network schemes: Eng Keong Lua, Ravi Sharma, Jon Crowcroft et al.
[iii] Wikipedia and telehash.org
[iv] Device Democracy: Saving the future of the Internet of Things
Additional references to be added prior to final publication.

Authors

Sanjay Panikkar
Sumabala Nair
Paul Brody
Veena Pureswaran

Contributors

John Cohn
Yunjung Chang
Gurvinder Ahluwalia
Peter Finn

Acknowlegements

Ethereum: Vitalik Buterin, Stephen Tual, Gavin Would
Telehash: Jeremie Miller
Samsung Electronics: President Hong, Dr. Jinsoo Yoon and the MSC Team
IBM Development Team: Amir Kamal, Hari Reddy, Nikhil Baxi, JungWon Cho

For additional information contact Veena Pureswaran at vpures@us.ibm.com

