區塊鏈: IBM/SAMSUNG ADEPT FOR IOT BLOCKCHAIN

Reyer Chu
20180723

ADEP (Autonomous DEcentralized P2P Telemetry) by IBM & Samsung

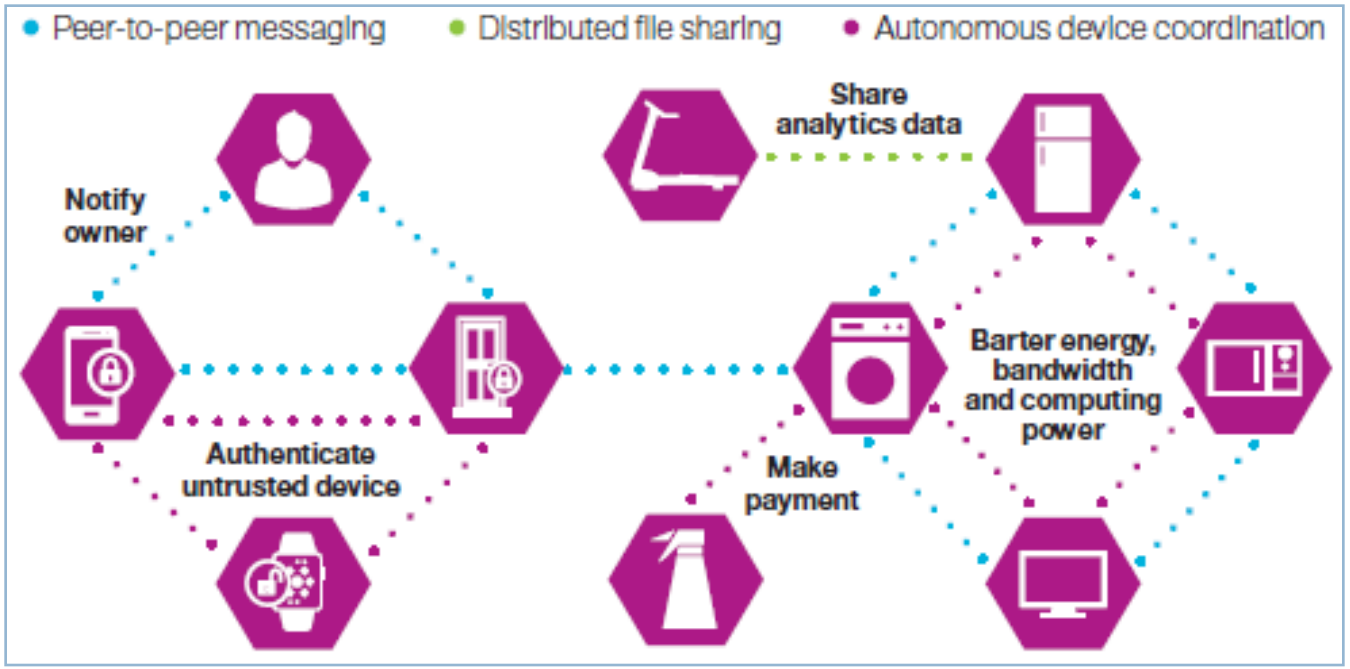
- 在2015年於賭城拉斯維加斯Las Vegas 舉辦的CES展覽中，IBM發表了一篇物聯網的概念驗證（Proof of Concept）: ADEPT 自律分散點對點網路遙測，是一個由IBM與韓國三星合作開發的物聯網系統，也是一個以類似比特幣的塊鏈機制為基礎的分散式物聯網。

M2M Protocol

- 與傳統物聯網的概念不同的地方是秩序並不是由一個中央系統來維持，而是由每一個裝置共同出力達成的協議
  - 裝置們之間建立了默契，能紋絲不亂的知道溝通的先後順序
  - Eg. 家電產品可以發出系統操作錯誤問題的信號並自行獲取軟體更新升級
  - Eg. 裝置可以透過ADEPT與其他周遭的同伴對電源需求進行討價還價，這對提升能源效率有極大的幫助

3 Foundational Functions by Using 3 Open-Source Protocols

1. P2P messaging: TeleHash
2. Distributing file sharing: BitTorrent
3. Autonomous device coordination: Ethereum smart-contract



1. P2P Messaging: TeleHash

- P2P messaging in a decentralized IoT must support:
  - Trustless, encrypted messaging and transport
  - Low latency with guaranteed delivery
  - Storage and forwarding of messages with "hop-on" to other connected devices
- Distributed Hash Table (DHT)
  - Enable peers to search for other peers on the network using a hash table with (key, value) pairs stored in DHT

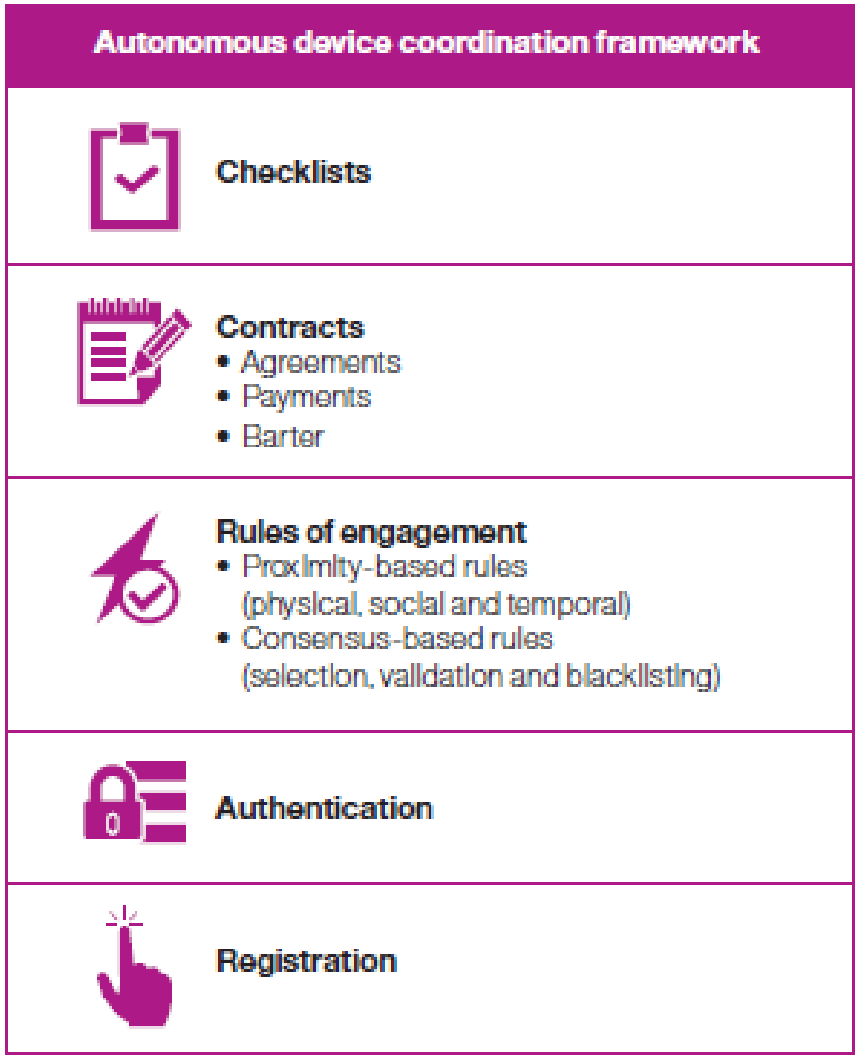
  ➔ Each device can generate its own unique public-key-based address (a hashname) to send & receive encrypted messages w/ other endpoints.
- TeleHash: Open source DHT of Kademlia protocol

2. Distributing File Sharing: BitTorrent

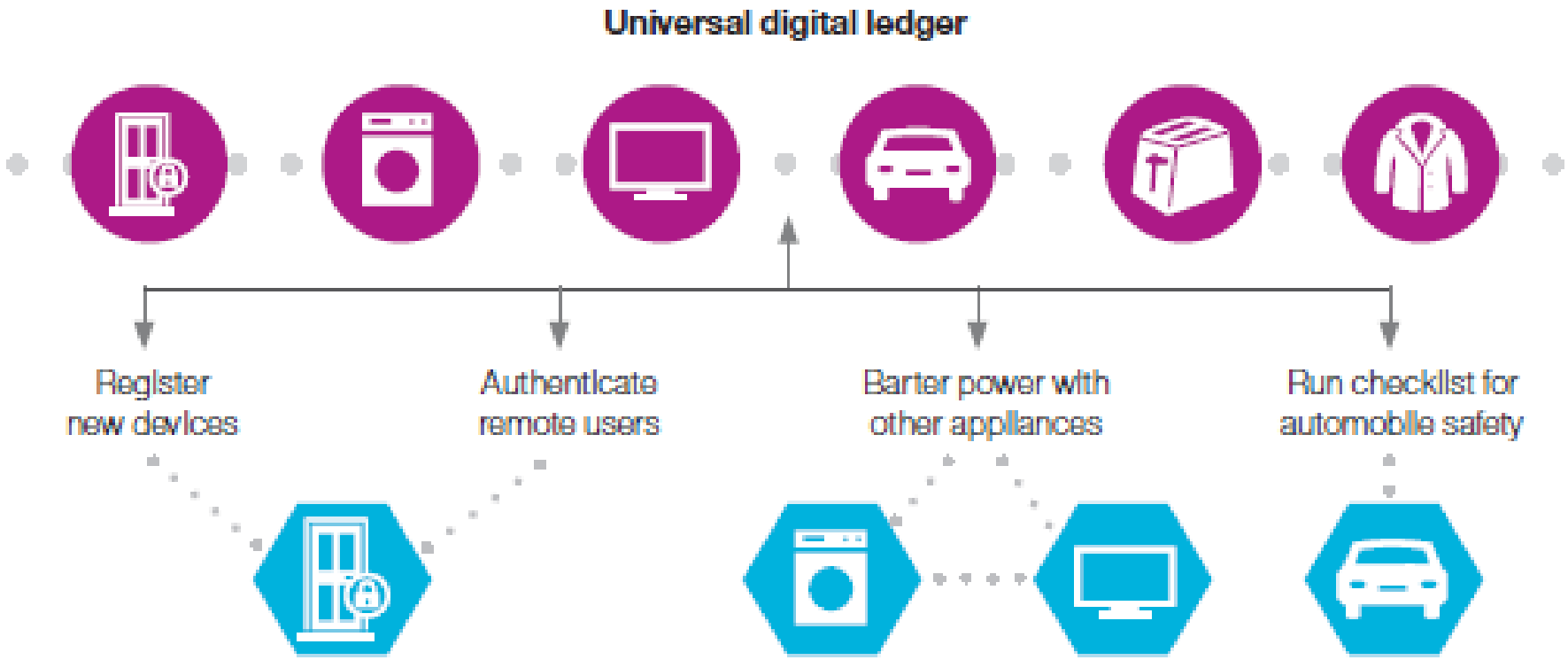
- Usage
  - Propagate software/firmware updates
  - Transfer device analytics report and media content
- Such distributed file sharing can also be achieved securely via distributed P2P networks using DHT.

3. Autonomous Device Coordination: Ethereum

- Empowers owners of devices to define & manage their own interactions
- Usage
  - Registration & authentication
  - Complex interactions: Owners define rules of engagement
    - Proximity-based (physical, social or temporal)
    - Consensus-based (selection, validation or blacklisting)
    - Triggered by other device
  - Contract
    - Simple agreements about actions or control
    - Complex financial contracts involving payments or barter
    - Digital checklists: Allow devices to maintain themselves to prevent failure



Blockchain For Various IoT Transactions

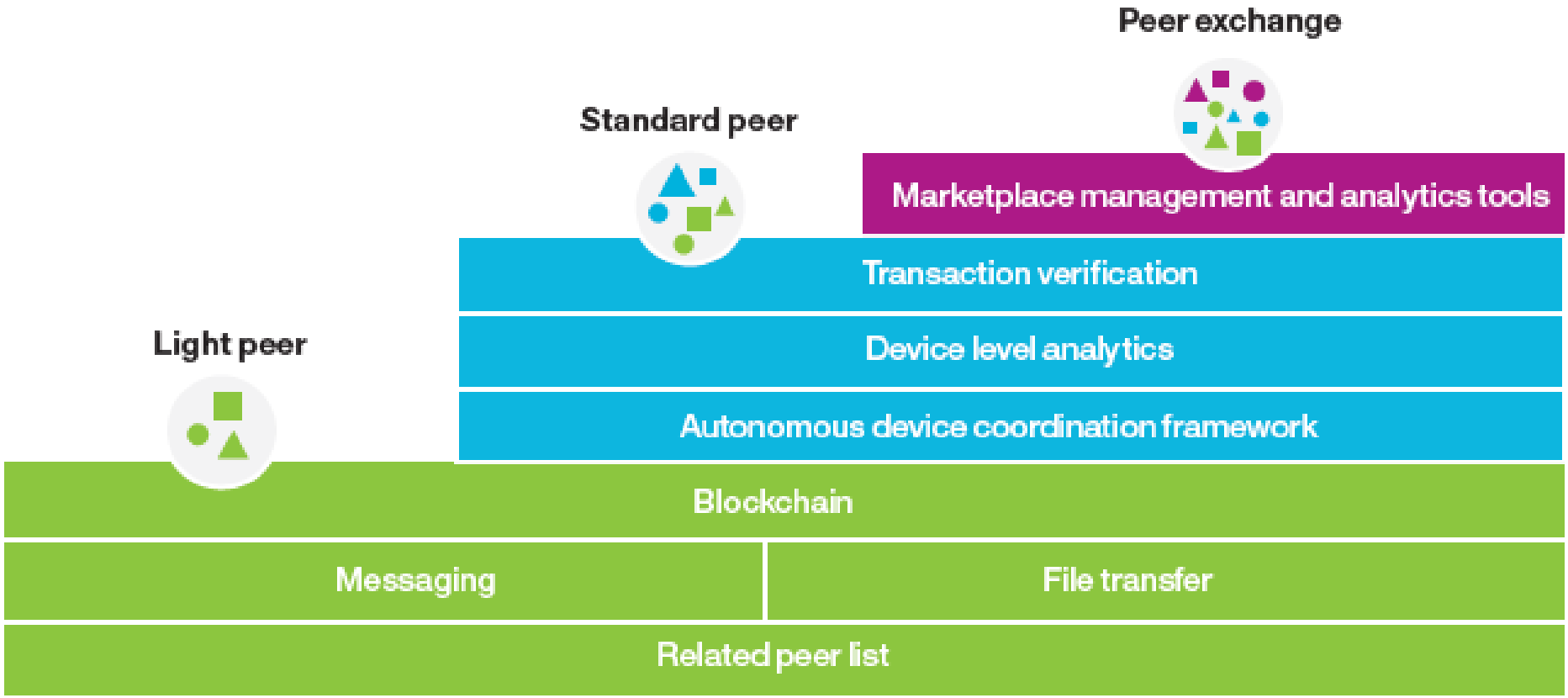


ADEPT Peer Architecture

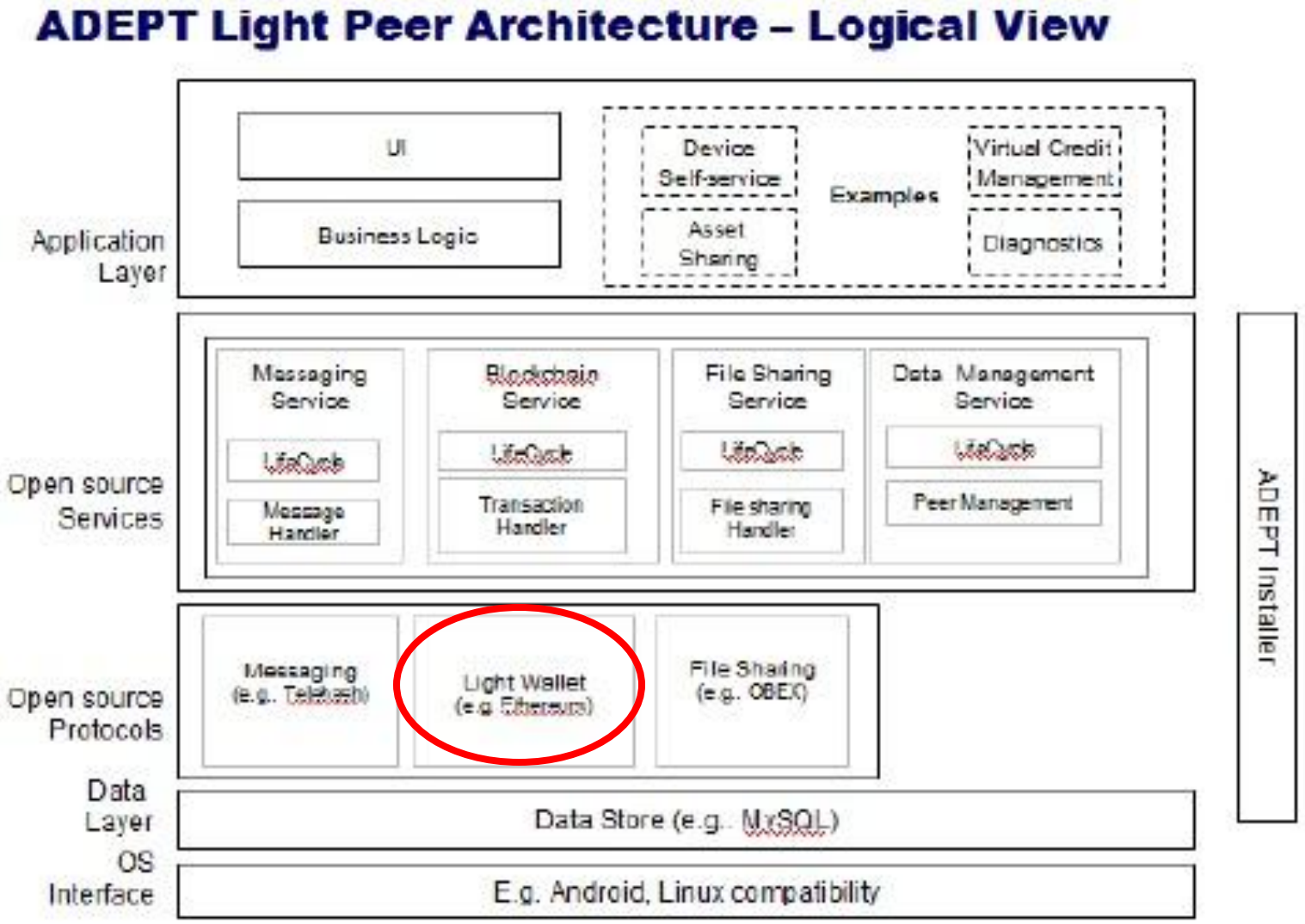
- Many tiny devices may not have full computational power and memory to manage complete blockchain
- 3 device types w/ 3 levels of capability
  - Light peer
  - Standard peer
  - Peer exchange (High-end device)

3 Device Types

- Device capabilities get increasingly from light peers to standard peers to peer exchanges

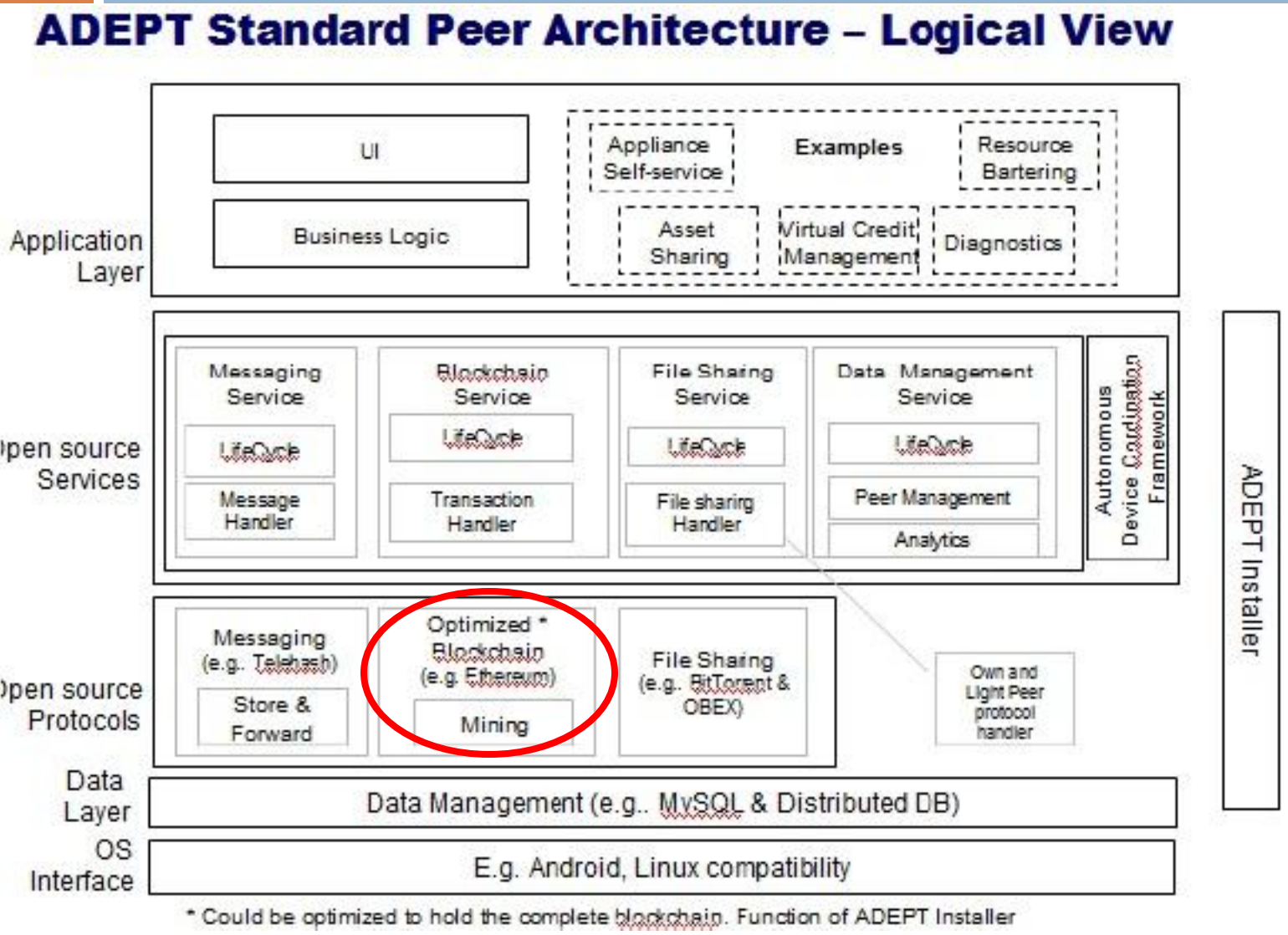


ADEP: Light Peer Architecture



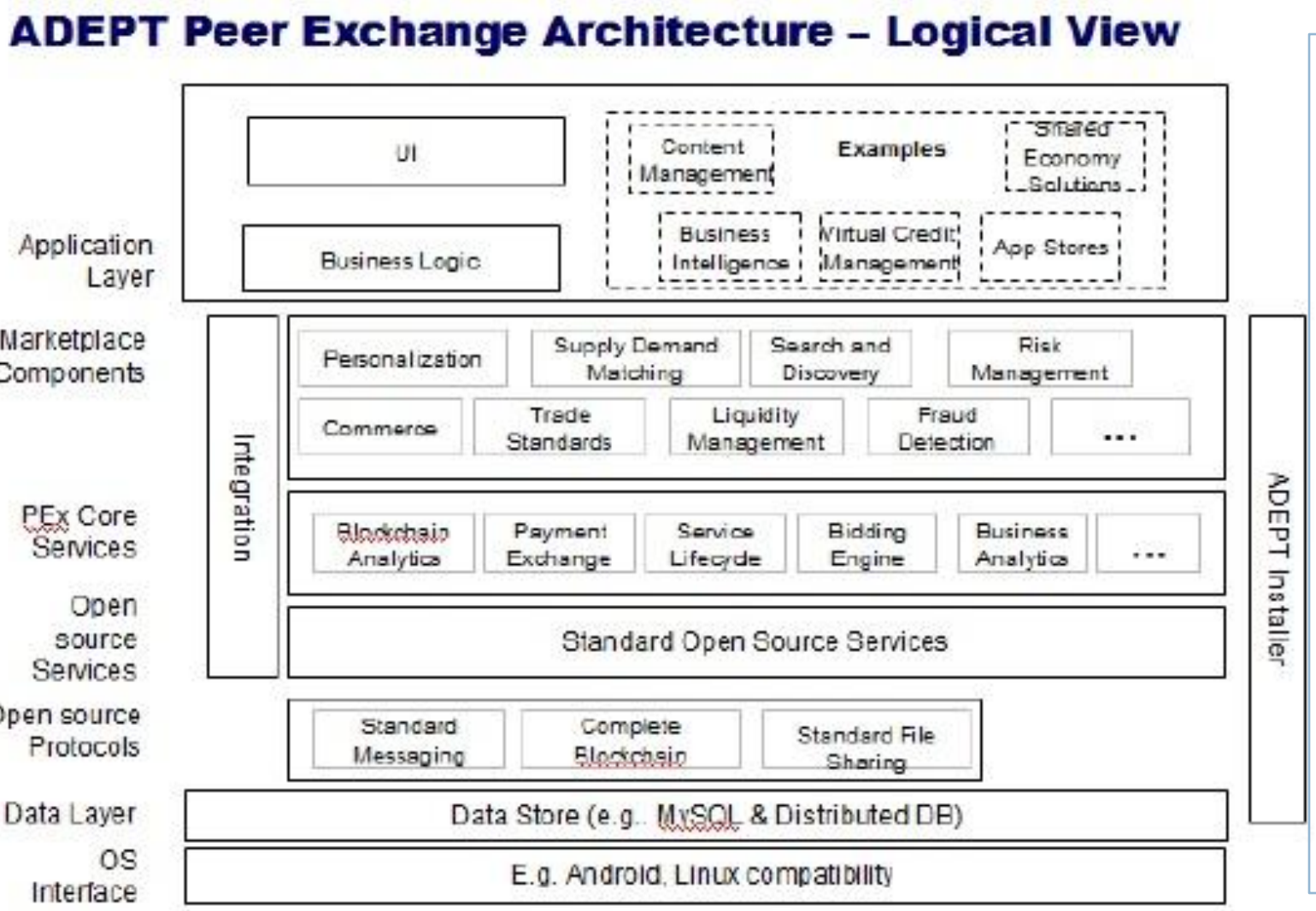
- No capability to store blockchains
- Only retain its own blockchain address and balance inside the device (i.e. light wallet)

ADEP: Standard Peer Architecture



- Can hold blockchain information for a certain period of time
- Can retain a part of blockchain based on its capabilities (e.g. Recent transactions for itself or other lighter devices)

ADEP: Peer Exchange Architecture

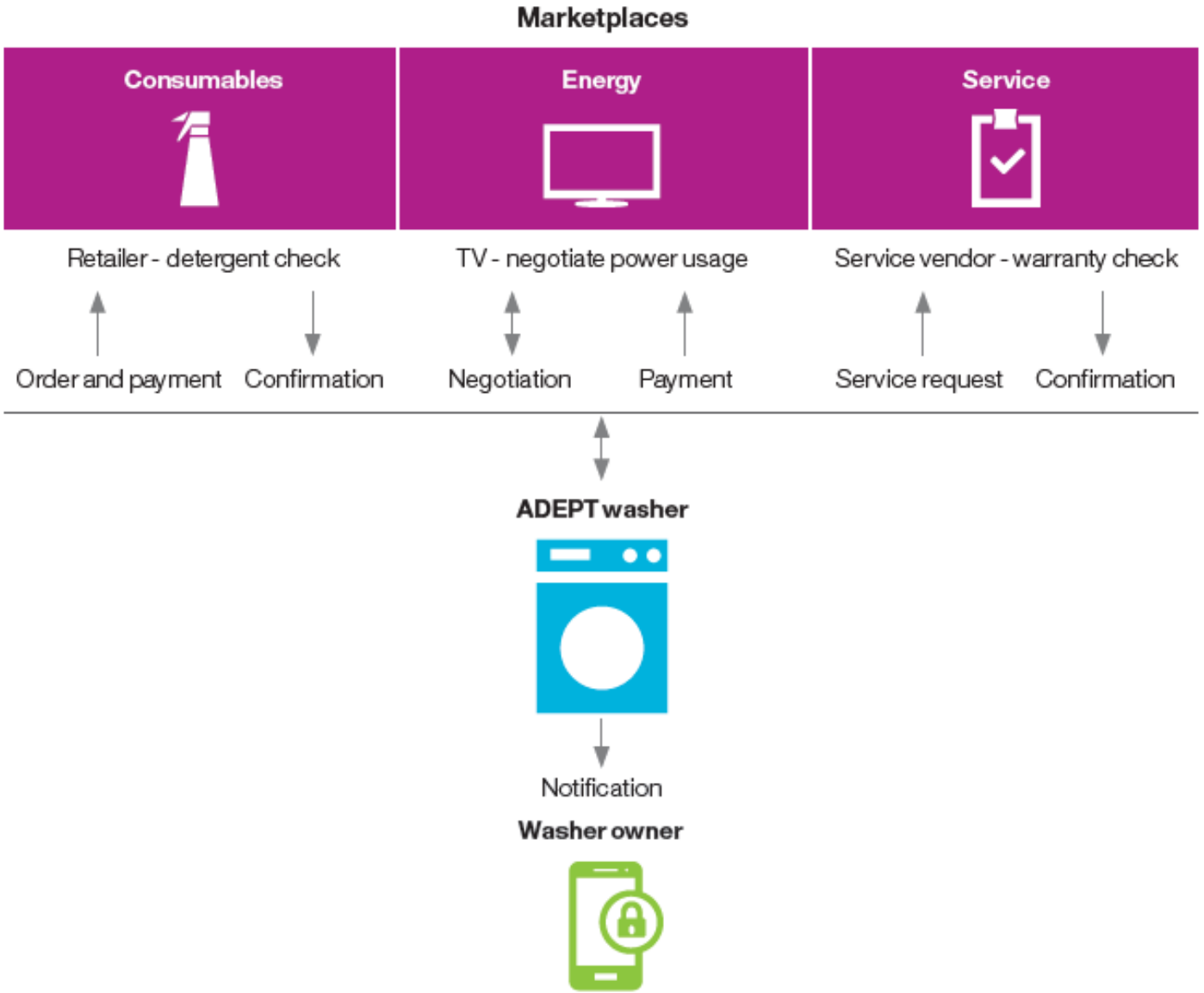


- High end devices w/ vast compute and storage capabilities
- Can have a complete copy of blockchain and analytical services

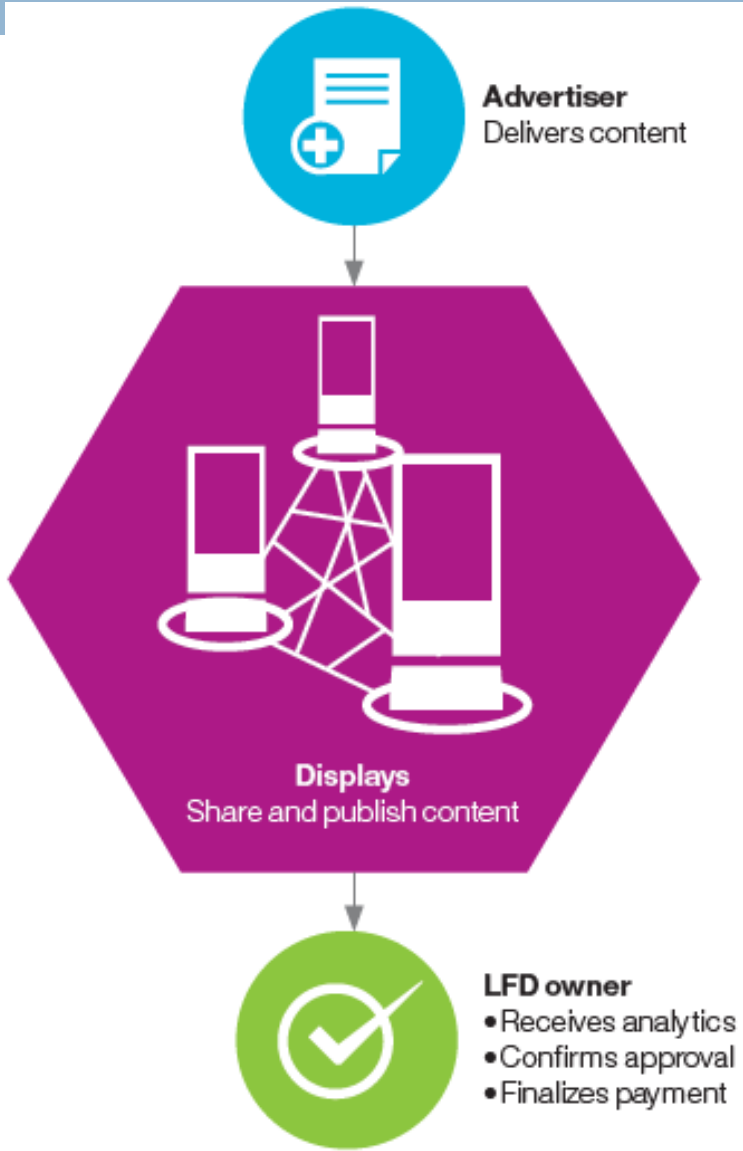
Marketplaces Hosted by Peer Exchanges

- Provide liquidity for transactions between devices

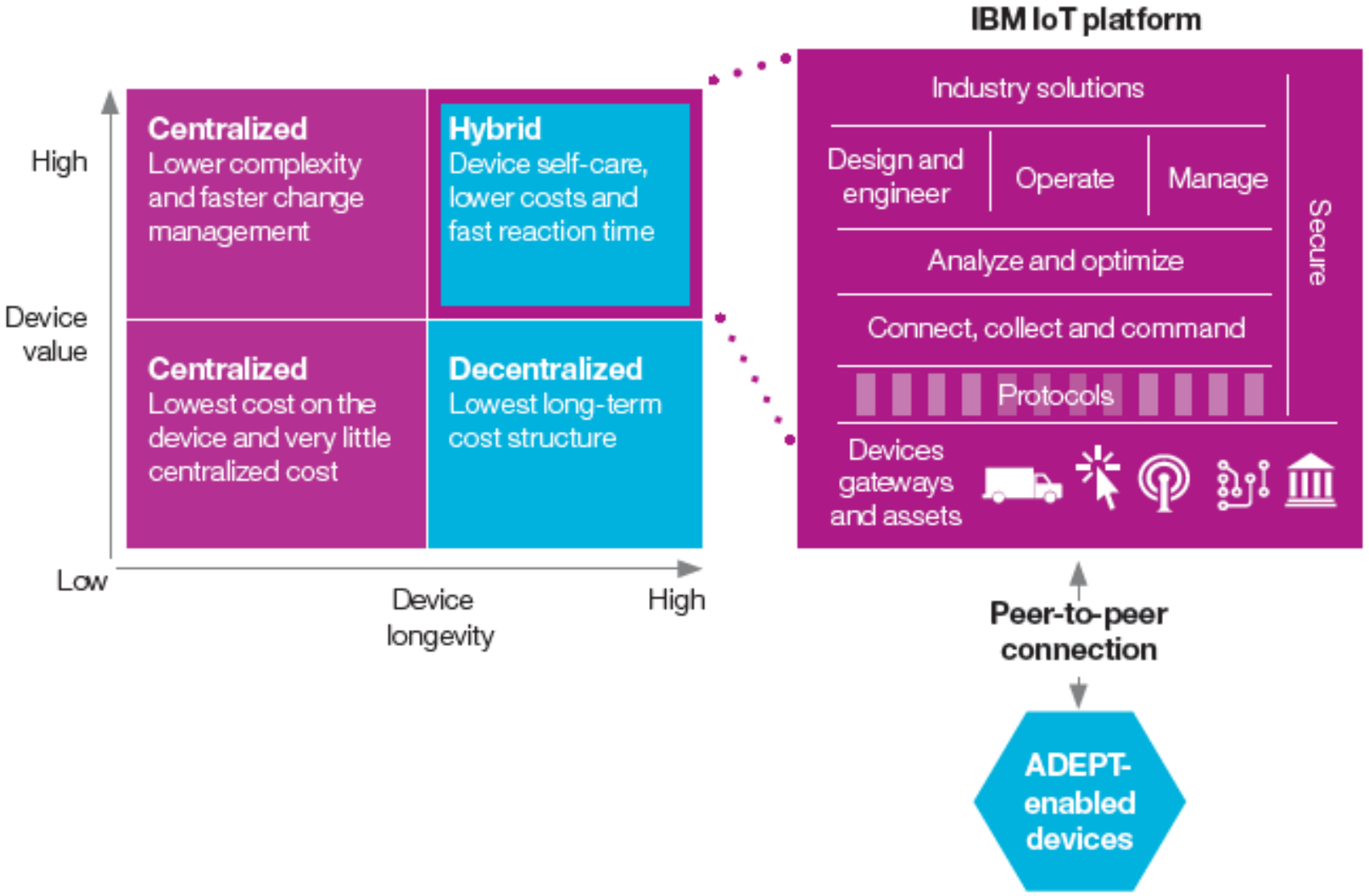
Marketplace Example 1: ADEPT Washer



Marketplace Example 2: Decentralized Advertising



Feasibility of ADEPT



Recommendations

- Augment centralized with decentralized
  - Low-cost, high-longevity device applications are good candidates to begin the expansion to a more hybrid IoT.
  - Industries where services are tightly controlled and economies that incur massive infrastructure costs from digitization are likely to benefit most from a hybrid model.
- Collaborate for change
  - This report: A functional PoC of a decentralized IoT
  - Actively engage with the IoT and blockchain communities to take critical steps to address these challenges
- Act now (w/ some issues)
  - Scalability challenges associated with commercializing distributed systems
  - Security
  - Coordination
  - Intellectual property management
  - Identity and privacy issues

References

- Empowering the edge - Practical insights on a decentralized Internet of Things
- IBM打造的物聯網實例：一台會買洗衣粉的洗衣機
- IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things
- IBM ADEPT Practictioner Perspective
- Distributed Hash Table (DHT)
- YouTube: Whitepaper Circle: IBM Adept - Presented by Graham Hughes

ADEPT by IBM & Samsung

- ADEPT: Autonomous DEcentralized P2P Telemetry (遙測)
  - Use PoW and PoS to secure transactions
- IoT device can be registered by manufacturer, dealer or end customer into a universal or regional blockchain representing its beginning of life.
- Once registered, it remains a unique entity within 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 blockchain can become the trusted product database.
  - E.g. 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.
  - ➔ 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

PoW For Smart Contract on a Blockchain by IBM

- A method to determine a PoW via a device by using a **predefined** set of nonce values.

- Background
  - Properties of IoT device:
    - Limited computational power & storage
    - Can be target for sophisticated hackers
      - Malicious participants may manipulate smart contracts.

➔ Limited PoW system to provide **equal chances** of successful completion of PoW to all IoT devices in the network

簡單講...

- 每個 IoT device 的 nonce 只允許用**特定子集**內的數值
  - → 讓每個 IoT device 有同等的機會挖到礦
  - → 單一 IoT device 不斷增加算力, 並無法增加挖到礦的機會
  - 可避免
    - 在 IoT network 中 device 為了挖到更多的礦而不斷增加算力
    - 外部有人意圖用龐大算力來控制區塊鏈
- IBM 提出一個系統性的方式建出 nonce 集
  - **每個 IoT device**

    1) 從特定數量的舊量測區塊 (EMB) 中,

    2) 取出部分具亂度的資料項,

    3) 導出 (D2N) 合法的 nonce 集
- 應用: IBM 設想其用在 smart contract for
  - 能源網路, 物流 (logistic) 網路
  - 群眾外包 (crowd-sourced) 氣象網路

Example

- EMB
  - Eligible measurement block
  - E.g. 前24小時生成的 measurement blocks
- D2N
  - Data to nonce transformation
  - D2N(data in EMB) → nonce
  - E.g. 4 LSBs
- NRB
  - Nonce reference block
  - = PoW 的 nonce 所對應的 EMB
  - E.g. If nonce = 0110 ➔ NRB = MB-ID4 IoT ID1

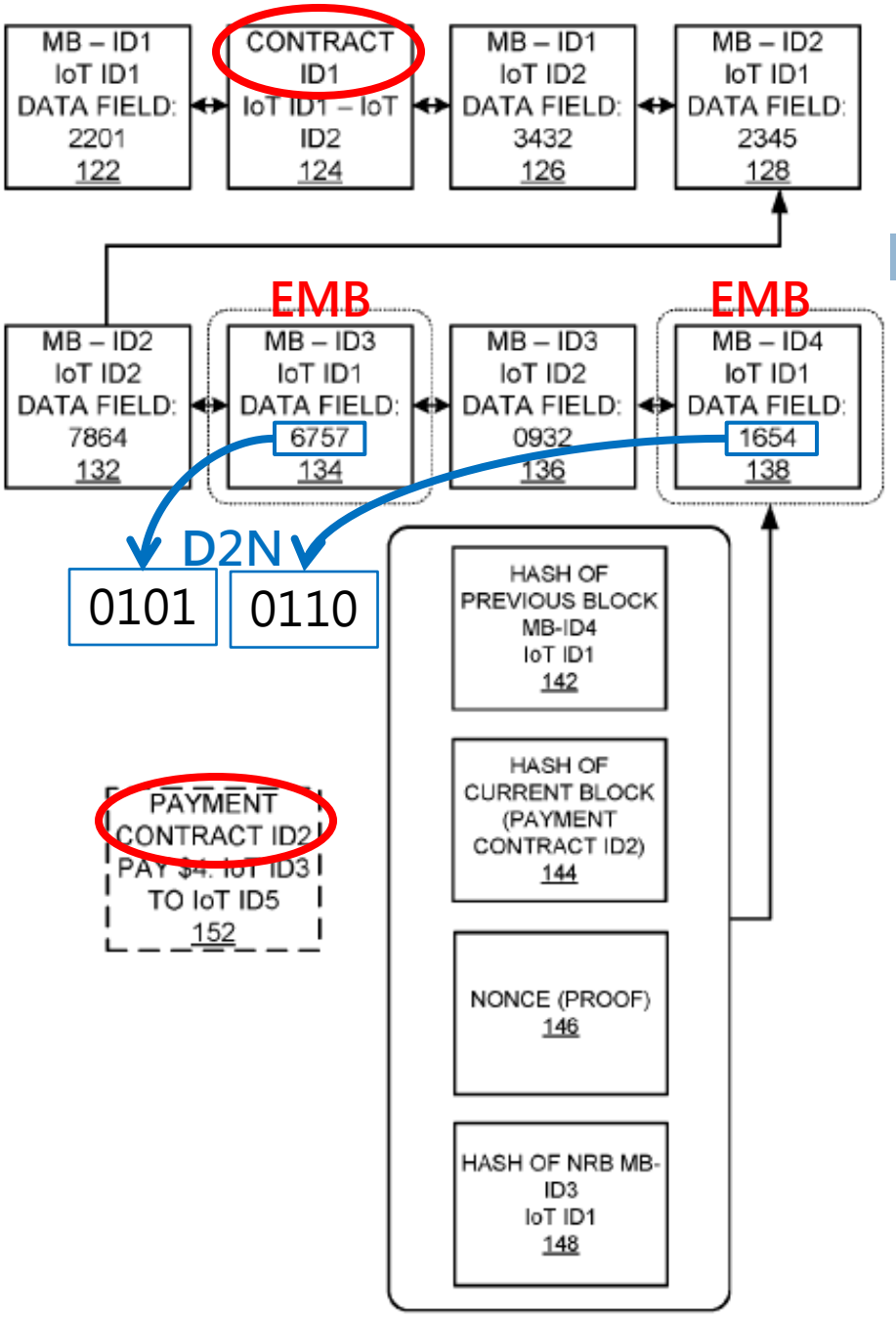


FIG. 1

Signaling Diagram

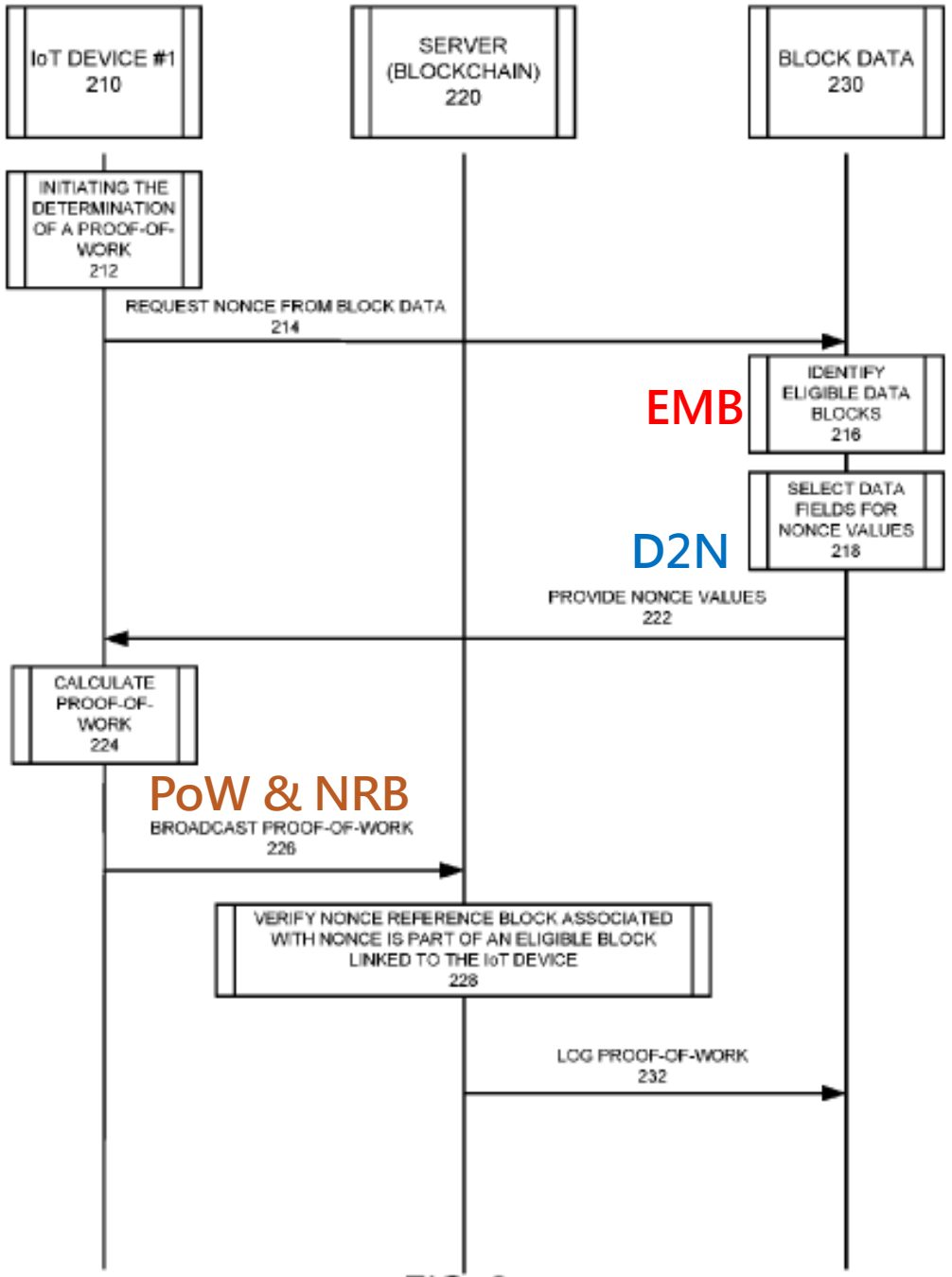
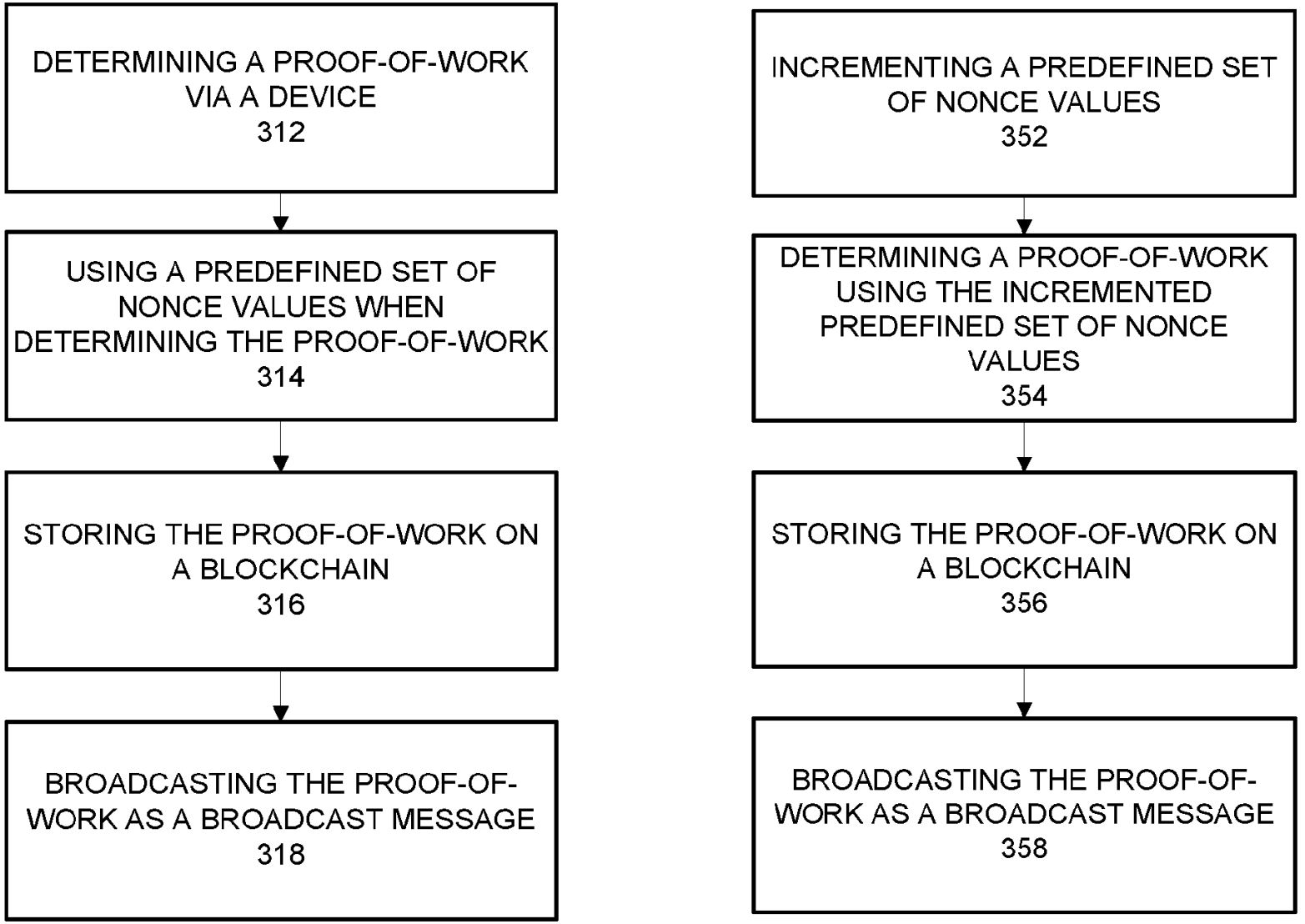


FIG. 2

Flow Diagram



System Block Diagram