區塊鏈: IBM PATENT FOR IOT BLOCKCHAIN

Reyer Chu
20180709

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

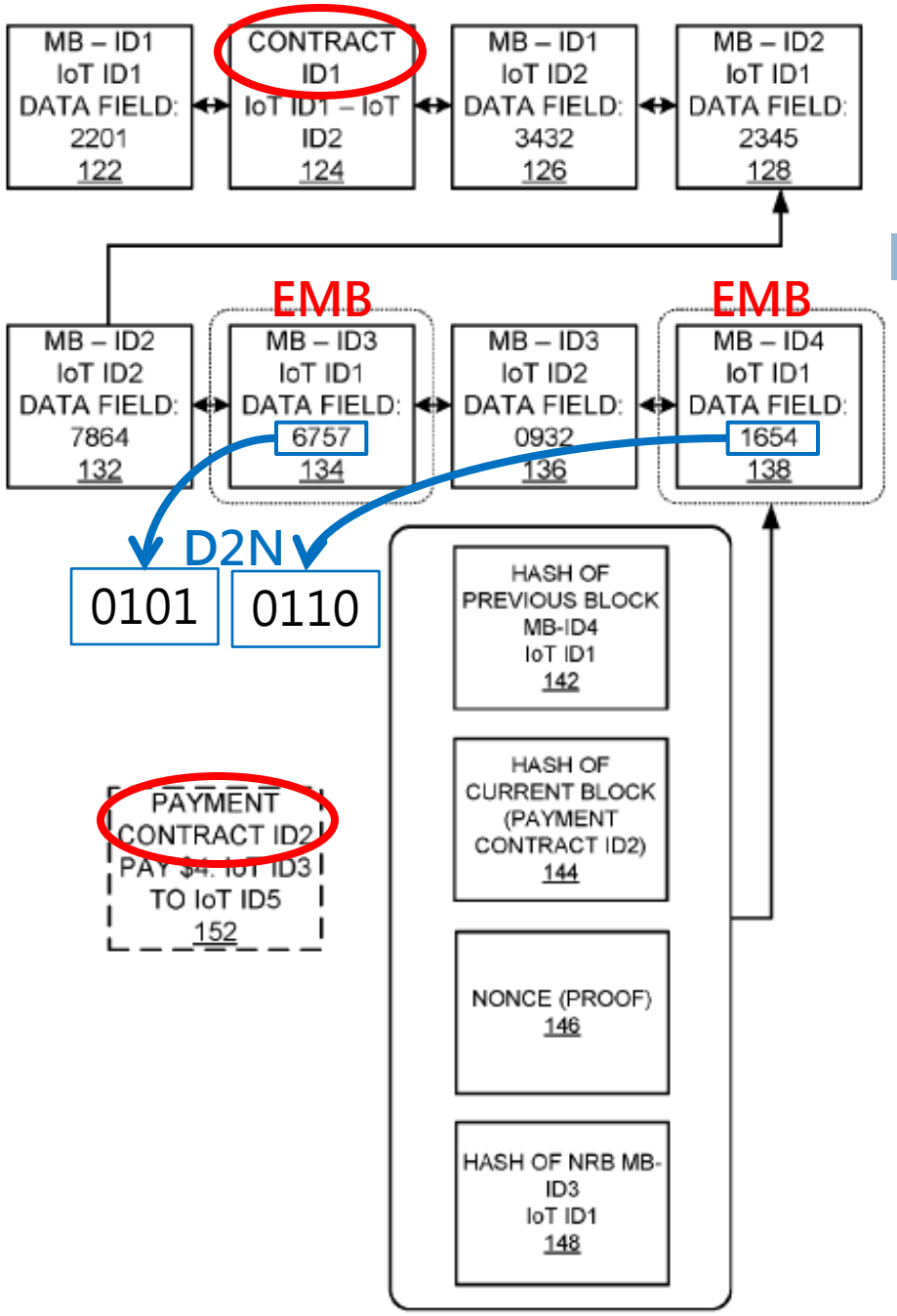


FIG. 1

Signaling Diagram

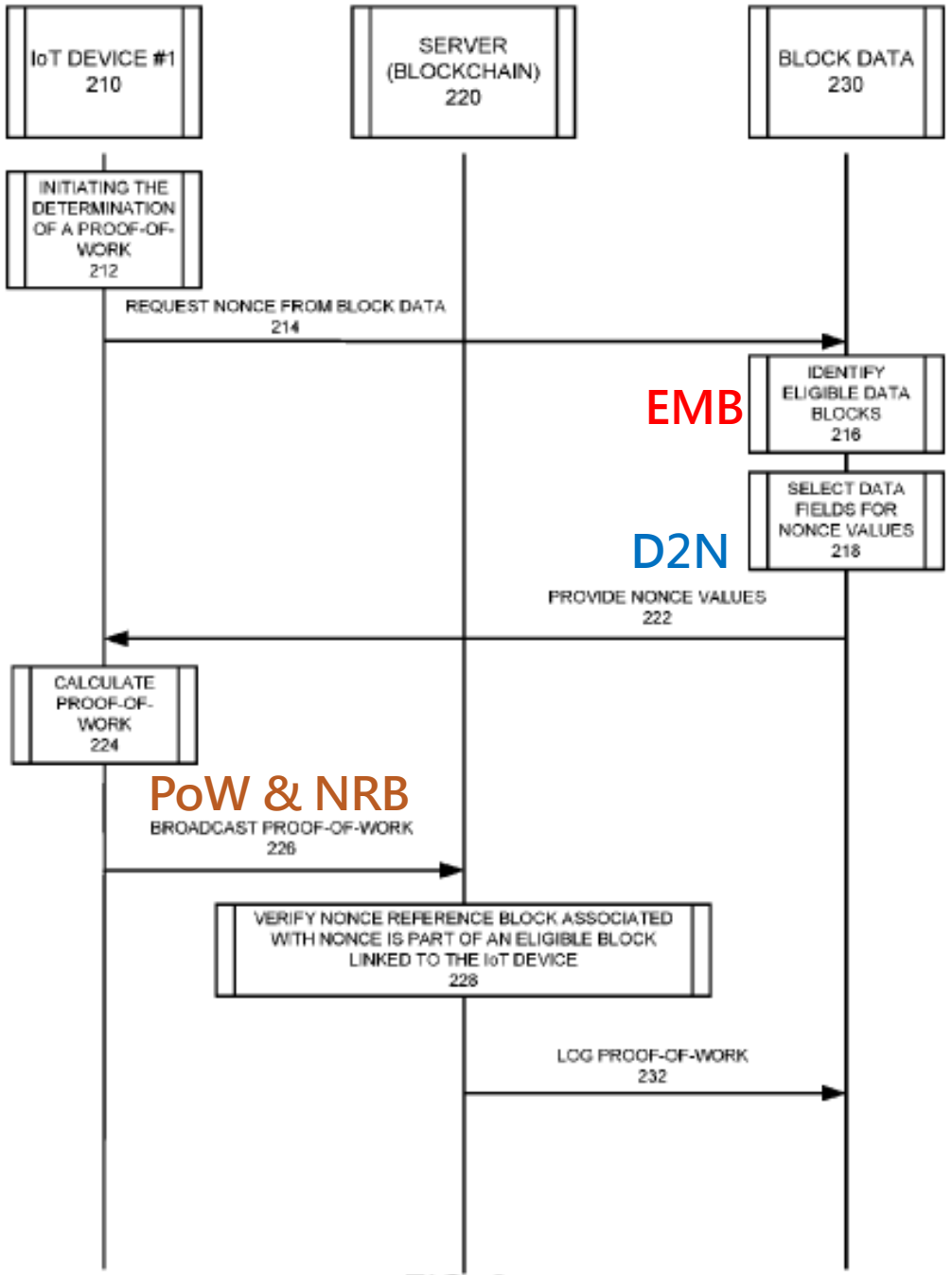
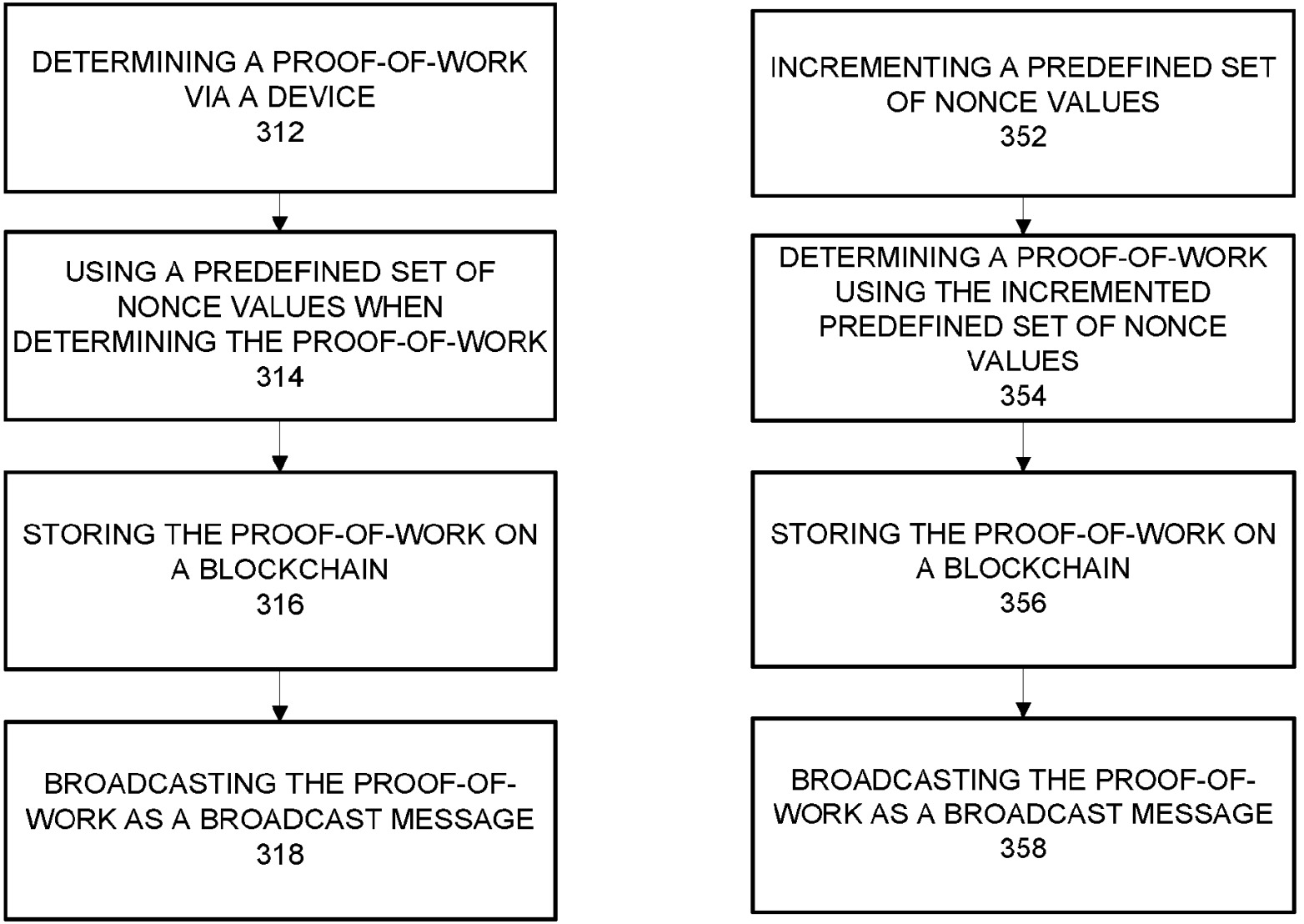
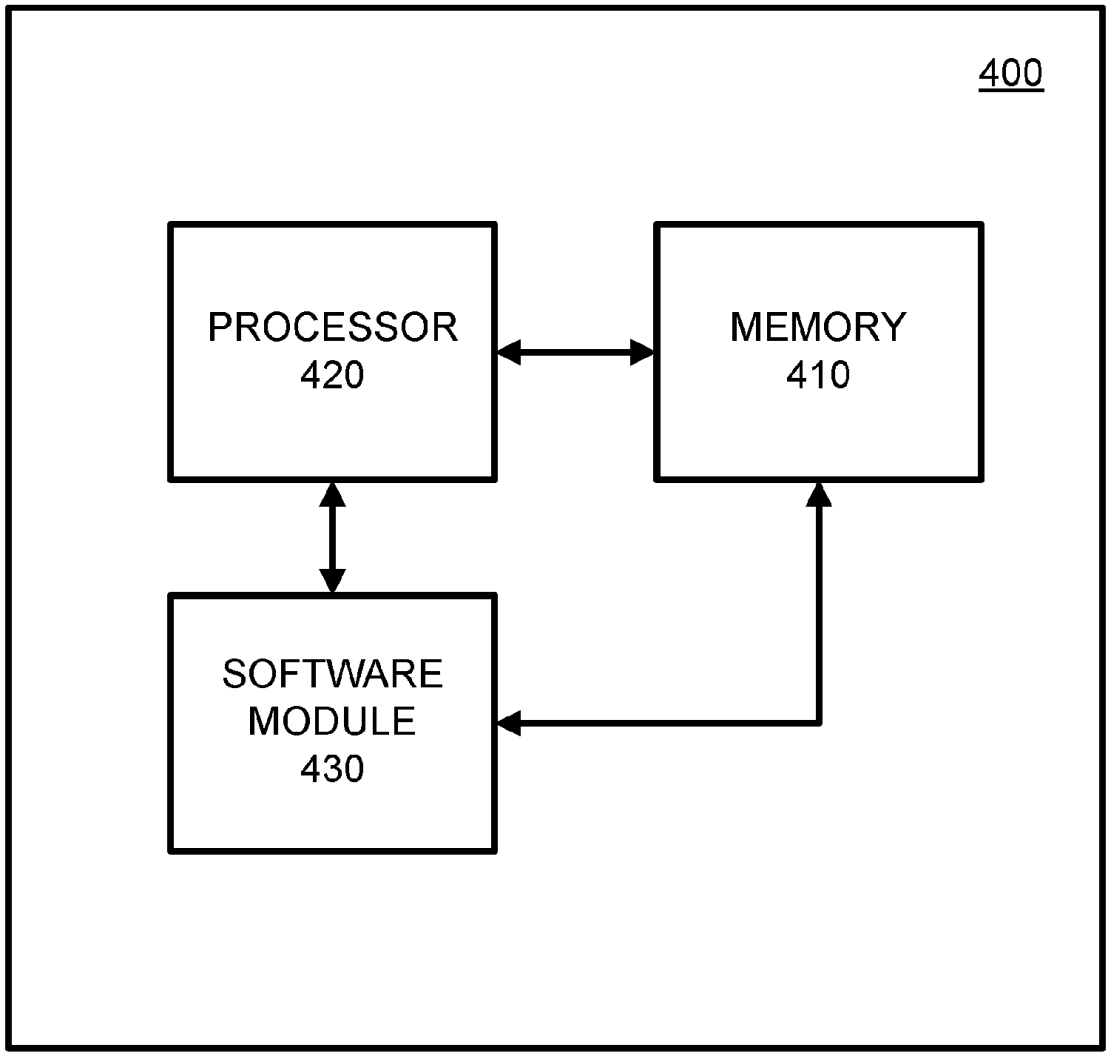


FIG. 2

Flow Diagram



System Block Diagram



References

- ADEP (Autonomous DEcentralized P2P Telemetry) by IBM & Samsung

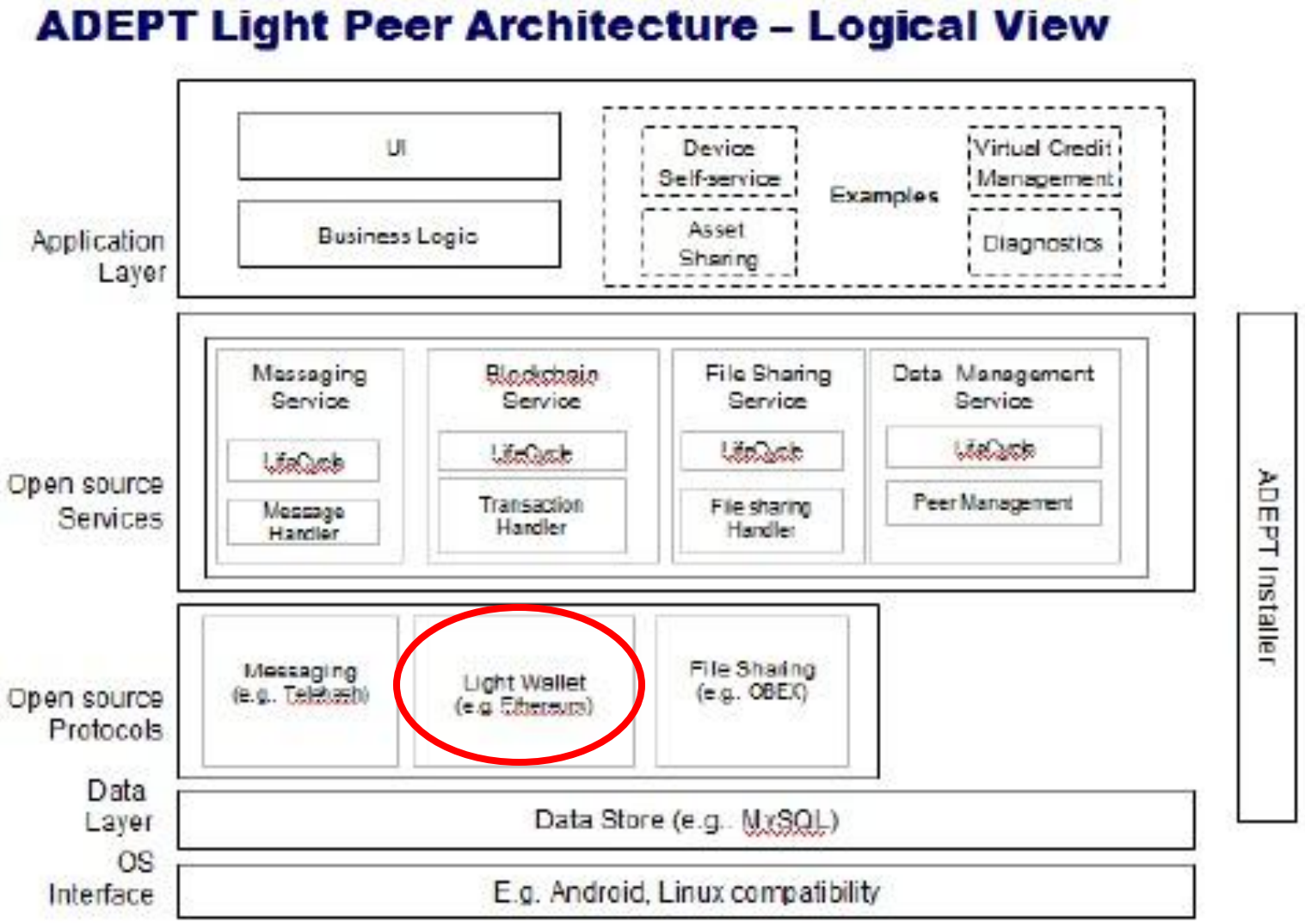
ADEPT by IBM & Samsung

- 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

ADEPT Peer Architecture

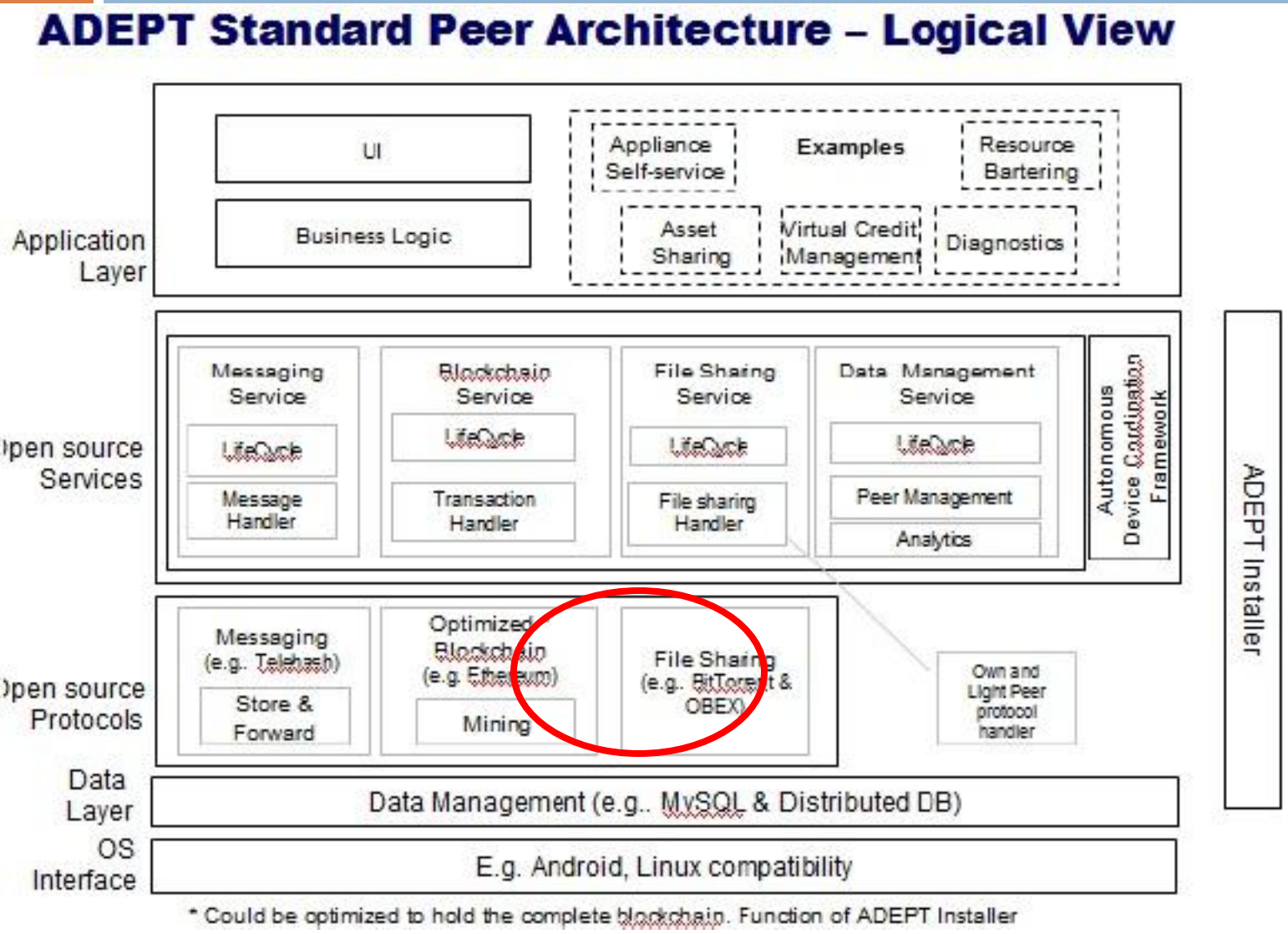
- Many tiny devices may not have full computational power and memory to manage complete blockchain
- 3 levels of capability
  - Light peer
  - Standard peer
  - Peer exchange (High-end device)

ADEP: Light Peer Architecture



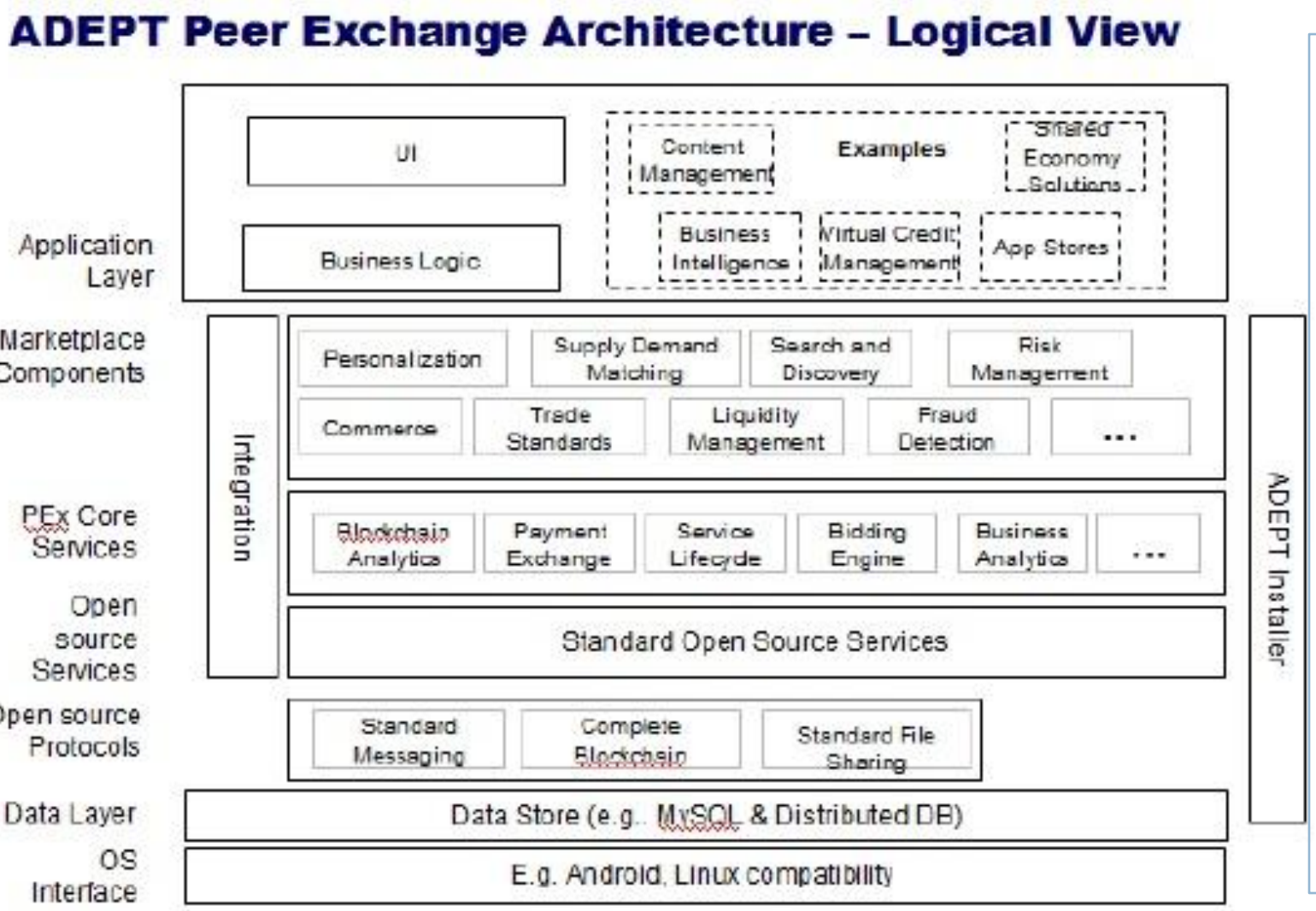
- No capability to store blockchains
- Only retain its own blockchain address and balance inside the device (i.e. light wallet)

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