Blockchain use cases
Lecture goals

● Do you need a Blockchain?
  ○ Coin management system
  ○ Medical data preservation system
  ○ Sharing a parking spot

● Parking dApp scenario
  ○ Stakeholders analysis and goals
  ○ Use cases
  ○ Solution-oriented requirements
    ■ Data model
    ■ State model
    ■ Behavior model
  ○ Non-functional requirements
    ■ Access control model
Blockchain types

- **Permissionless / public**
  - Requires no permission to join the Blockchain network
  - Open to all and transactions are visible to everyone
  - More transparent but slow transactions speed

- **Permissioned**
  - Requires permissions to join the Blockchain network
  - Only pre-defined nodes can participate in consensus mechanism
  - Fast, privacy oriented but less transparent

- **Private / Hybrid**
  - Controls and network governance assigned to one designated authority
  - Blockchain activity is only visible to chosen participants
  - More privacy oriented, scalable but less decentralised
Blockchain platforms

Blockchain platforms are growing after the emergence of Bitcoin and smart contracts:

- **Bitcoin**
  - Purely a cryptocurrency platform, an example of permissionless Blockchain
- **Ethereum**
  - Decentralised applications (dApps), an example of permissionless Blockchain
- **Hyperledger-fabric**
  - Decentralised applications (dApps), an example of permissioned Blockchain
- **Corda**
  - Main focus on financial-based decentralised applications (dApps), an example of permissioned Blockchain
- **Multichain**
Do you need a Blockchain?

- Coin management system
- Medical data preservation system
- Sharing a parking spot
Do you need to store state?  

If NO, stop.  

If YES, go to next question.

Are there multiple writers?  

If NO, go to next question.  

If YES, go to next question.

Can you always use an online TTP?  

If NO, go to next question.  

If YES, go to next question.

Are all writers known?  

If NO, go to next question.  

If YES, go to next question.

Are all writers trusted?  

If NO, stop.  

If YES, go to next question.

Is public verifiability required?  

If NO, stop.  

If YES, go to next question.

Ethereum (Permissionless Blockchain)  

Hyperledger (Permissioned Blockchain)  

Multichain (Private Permissioned Blockchain)  

Don’t use Blockchain

Wüst K. and Gervais A. (2017) Do you need a Blockchain?  
Do you need a Blockchain?

- *Coin management system*
- Medical data preservation system
- Sharing a parking spot
Coin management system

- **Coin management**
  - Add, View, update, delete
- **Coin history management**
  - Add, View, update, delete
- **Other details**
Do you need to store state?

- Are there multiple writers?
  - NO
  - Are there multiple writers?
    - NO
    - Are all writers known?
      - NO
      - Are all writers trusted?
        - NO
        - Is public verifiability required?
          - NO
          - Multichain
            - (Private Permissioned Blockchain)
          - YES
          - Hyperledger
            - (Permissioned Blockchain)
        - YES
        - Ethereum
          - (Permissionless Blockchain)
      - YES
      - Is public verifiability required?
        - NO
        - Multichain
          - (Private Permissioned Blockchain)
        - YES
        - Hyperledger
          - (Permissioned Blockchain)
    - NO
    - Can you always use an online TTP?
      - NO
      - Are all writers known?
        - NO
        - Are all writers trusted?
          - NO
          - Is public verifiability required?
            - NO
            - Multichain
              - (Private Permissioned Blockchain)
            - YES
            - Hyperledger
              - (Permissioned Blockchain)
          - YES
          - Ethereum
            - (Permissionless Blockchain)
        - YES
        - Is public verifiability required?
          - NO
          - Multichain
            - (Private Permissioned Blockchain)
          - YES
          - Hyperledger
            - (Permissioned Blockchain)
      - YES
      - Is public verifiability required?
        - NO
        - Multichain
          - (Private Permissioned Blockchain)
        - YES
        - Hyperledger
          - (Permissioned Blockchain)
    - YES
    - Is public verifiability required?
      - NO
      - Multichain
        - (Private Permissioned Blockchain)
      - YES
      - Hyperledger
        - (Permissioned Blockchain)
  - YES
  - Can you always use an online TTP?
    - NO
    - Are all writers known?
      - NO
      - Are all writers trusted?
        - NO
        - Is public verifiability required?
          - NO
          - Multichain
            - (Private Permissioned Blockchain)
          - YES
          - Hyperledger
            - (Permissioned Blockchain)
        - YES
        - Is public verifiability required?
          - NO
          - Multichain
            - (Private Permissioned Blockchain)
          - YES
          - Hyperledger
            - (Permissioned Blockchain)
      - YES
      - Is public verifiability required?
        - NO
        - Multichain
          - (Private Permissioned Blockchain)
        - YES
        - Hyperledger
          - (Permissioned Blockchain)
    - YES
    - Is public verifiability required?
      - NO
      - Multichain
        - (Private Permissioned Blockchain)
      - YES
      - Hyperledger
        - (Permissioned Blockchain)

- Coin management
  - Add, View, update, delete
- Coin history management
  - Add, View, update, delete
- Other details
Do you need to store state?

YES
Are there multiple writers?
NO

YES
Can you always use an online TTP?
NO

YES
Are all writers known?
NO

Ethereum
(Permissionless Blockchain)

Hyperledger
(Permissioned Blockchain)

Multichain
(Private Permissioned Blockchain)

Don’t use Blockchain

Is public verifiability required?
YES

NO

● Coin management
  ○ Add, View, update, delete

● Coin history management
  ○ Add, View, update, delete

● Other details
- Coin management
  - Add, View, update, delete
- Coin history management
  - Add, View, update, delete
- Other details

Choose the appropriate blockchain:

- Ethereum (Permissionless Blockchain)
- Hyperledger (Permissioned Blockchain)
- Multichain (Private Permissioned Blockchain)
- Don't use Blockchain
Do you need to store state?

Are there multiple writers?

Can you always use an online TTP?

Are all writers known?

Is public verifiability required?

Ethereum (Permissionless Blockchain)

Hyperledger (Permissioned Blockchain)

Multichain (Private Permissioned Blockchain)

Don’t use Blockchain

- Coin management
  - Add, View, update, delete
- Coin history management
  - Add, View, update, delete
- Other details
Do you need a Blockchain?

- Coin management system
- Medical data preservation system
- Sharing a parking spot
Do you need a Blockchain?

[Wüst an Gervais, 2017]

Medical data preservation system

- **Data operations**
  - Store & query data
  - Prevent medical data from being tampered, forged or deleted

- **Multiples writers**
  - System should be more transparent

- **Disintermediate**

---

Do you need to store state?

- **Data operations**
  - Store & query data
  - Prevent medical data from being tampered, forged or deleted
- **Multiples writers**
  - System should be more transparent
- **Disintermediate**

Ethereum (Permissionless Blockchain)

Hyperledger (Permissioned Blockchain)

Multichain (Private Permissioned Blockchain)

Don't use Blockchain
Do you need to store state?

- **YES**
  - Are there multiple writers?
    - **YES**
      - Can you always use an online TTP?
        - **NO**
          - Are all writers known?
            - **NO**
              - Are all writers trusted?
                - **NO**
                  - Is public verifiability required?
                    - **YES**
                      - **Hyperledger** (Permissioned Blockchain)
                    - **NO**
                      - **Multichain** (Private Permissioned Blockchain)
                - **YES**
                  - **Ethereum** (Permissionless Blockchain)
            - **YES**
              - **Data operations**
                - ○ **Store & query data**
                - ○ **Prevent medical data from being tampered, forged or deleted**
              - **Multiples writers**
                - ○ System should be more transparent
              - **Disintermediate**
        - **YES**
          - **Data operations**
            - ○ **Store & query data**
            - ○ **Prevent medical data from being tampered, forged or deleted**
          - **Multiples writers**
            - ○ System should be more transparent
          - **Disintermediate**
    - **NO**
      - **NO**
        - **NO**
          - **NO**
            - **NO**
              - **NO**
                - **NO**
                  - **NO**
                    - **NO**
                      - **NO**
                        - **NO**
                          - **NO**
                            - **NO**
                              - **NO**
                                - **NO**
                                  - **NO**
                                    - **NO**
                                      - **NO**
                                        - **NO**
                                          - **NO**
                                            - **NO**
                                              - **NO**
                                                - **NO**
                                                  - **NO**
                                                    - **NO**
                                                      - **NO**
                                                        - **NO**
                                                          - **NO**
                                                            - **NO**
                                                              - **NO**
                                                                - **NO**
                                                                  - **NO**
                                                                      - **NO**
                                                                        - **NO**
                                                                          - **NO**
                                                                            - **NO**
                                                                             - **NO**
                                                                              - **NO**
                                                                                - **NO**
                                                                                  - **NO**
                                                                                      - **NO**
                                                                                       - **NO**
                                                                                        - **NO**
                                                                                           - **NO**
                                                                                            - **NO**
                                                                                               - **NO**
                                                                                                - **NO**
                                                                                                    - **NO**
                                                                                                      - **NO**
                                                                                                       - **NO**
                                                                                                         - **NO**
                                                                                                          - **NO**
                                                                                                             - **NO**
                                                                                                               - **NO**
                                                                                                                  - **NO**
                                                                                                                     - **NO**
                                                                                                                       - **NO**
                                                                                                                          - **NO**
                                                                                                                              - **NO**
                                                                                                                                - **NO**
                                                                                                                                    - **NO**
                                                                                                                                        - **NO**
                                                                                                                                             - **NO**
                                                                                                                                               - **NO**
                                                                                                                                                       - **NO**
                                                                                        -  **Don’t use Blockchain**
Do you need to store state?

Yes

Are there multiple writers?

No

Can you always use an online TTP?

Yes

Are all writers known?

No

Are all writers trusted?

Yes

Is public verifiability required?

No

Ethereum
(Permissionless Blockchain)

No

Hyperledger
(Permissioned Blockchain)

No

Multichain
(Private Permissioned Blockchain)

Yes

Data operations
- Store & query data
- Prevent medical data from being tampered, forged or deleted

Multiples writers
- System should be more transparent

Disintermediate

Don’t use Blockchain
● Data operations
  ○ Store & query data
  ○ Prevent medical data from being tampered, forged or deleted

● **Multiples writers**
  ○ **System should be more transparent**

● Disintermediate

Ethereum (Permissionless Blockchain)

Hyperledger (Permissioned Blockchain)

Multichain (Private Permissioned Blockchain)

Don’t use Blockchain
Do you need to store state?

- NO
- YES

Are there multiple writers?

- NO
- YES

Can you always use an online TTP?

- YES
- NO

Are all writers known?

- NO
- YES

Is public verifiability required?

- NO
- YES

- Ethereum (Permissionless Blockchain)
- Hyperledger (Permissioned Blockchain)
- Multichain (Private Permissioned Blockchain)
- Don’t use Blockchain

● Data operations
  ○ Store & query data
  ○ Prevent medical data from being tampered, forged or deleted

● Multiples writers
  ○ System should be more transparent

● Disintermediate
• **Data operations**
  ○ Store & query data
  ○ Prevent medical data from being tampered, forged or deleted

• **Multiples writers**
  ○ System should be more transparent

• **Disintermediate**
Do you need to store state?  

- **Yes**  
  - Are there multiple writers?  
    - **Yes**  
      - Can you always use an online TTP?  
        - **No**  
          - Are all writers trusted?  
            - **Yes**  
              - Is public verifiability required?  
                - **No**  
                  - Hyperledger (Permissioned Blockchain)  
                - **Yes**  
                  - Multichain (Private Permissioned Blockchain)  
            - **No**  
              - Don’t use Blockchain  
        - **Yes**  
          - Are all writers known?  
            - **No**  
              - Do you need to store state?  
                - **Yes**  
                  - Are there multiple writers?  
                    - **No**  
                      - Can you always use an online TTP?  
                        - **Yes**  
                          - Are all writers trusted?  
                            - **Yes**  
                              - Hyperledger (Permissioned Blockchain)  
                            - **No**  
                              - Multichain (Private Permissioned Blockchain)  
                        - **No**  
                          - Are all writers known?  
                            - **No**  
                              - Don’t use Blockchain  
                            - **Yes**  
                              - Ethereum (Permissionless Blockchain)  
          - **No**  
            - Data operations  
              - **Yes**  
                - Store & query data  
                  - System should be more transparent  
              - **No**  
                - Prevent medical data from being tampered, forged or deleted  
            - Multiples writers  
              - **Yes**  
                - System should be more transparent  
              - **No**  
                - Prevent medical data from being tampered, forged or deleted  
            - Disintermediate  
              - **Yes**  
                - System should be more transparent  
              - **No**  
                - Prevent medical data from being tampered, forged or deleted
Do you need to store state?

- NO

Are there multiple writers?

- NO

Can you always use an online TTP?

- NO

Are all writers known?

- NO

Are all writers trusted?

- NO

Is public verifiability required?

- YES

Data operations

- ● Store & query data
- ○ Prevent medical data from being tampered, forged or deleted

Multiples writers

- ● System should be more transparent

Disintermediate

- NO

Ethereum

(Permissionless Blockchain)

Hyperledger

(Permissioned Blockchain)

Multichain

(Private Permissioned Blockchain)

Don’t use Blockchain
Do you need a Blockchain?

- Coin management system
- Medical data preservation system
- *Sharing a parking spot*
Sharing a parking spot

- Track the states of parking spots
- Multiple parties
  - Parking spots owners & renters
- Disintermediate
- Known parking spots owners
Sharing a parking spot

- Track the states of parking spots
- Multiple parties
  - Parking spots owners & renters
- Disintermediate
- Known parking spots owners

Let’s take 2 minutes to think about what platform would be feasible
- Track the states of parking spots
- Multiple parties
  - Parking spots owners & renters
- Disintermediate
- Known parking spots owners
Do you need to store state?

- **YES**
  - Are there multiple writers?
    - **NO**
      - Can you always use an online TTP?
        - **NO**
          - Are all writers known?
            - **NO**
              - Are all writers trusted?
                - **NO**
                  - Is public verifiability required?
                    - **YES**
                      - **Ethereum** (Permissionless Blockchain)
                    - **NO**
                      - **Hyperledger** (Permissioned Blockchain)
            - **YES**
              - **Multichain** (Private Permissioned Blockchain)
        - **YES**
          - **Ethereum** (Permissionless Blockchain)
    - **YES**
      - **Hyperledger** (Permissioned Blockchain)
- **NO**
  - **NO**
    - **Multichain** (Private Permissioned Blockchain)
  - **YES**
    - **Don’t use Blockchain**

- **Track the states of parking spots**
- **Multiple parties**
  - Parking spots owners & renters
- **Disintermediate**
- **Known parking spots owners**
Do you need to store state?

Are there multiple writers?

Can you always use an online TTP?

Are all writers known?

Are all writers trusted?

Is public verifiability required?

- Track the states of parking spots
- Multiple parties
  - Parking spots owners & renters
- Disintermediate
- Known parking spots owners

Ethereum (Permissionless Blockchain)

Hyperledger (Permissioned Blockchain)

Multichain (Private Permissioned Blockchain)

Don’t use Blockchain
Do you need to store state?

- No

Are there multiple writers?

- Yes

Can you always use an online TTP?

- No

Are all writers known?

- Yes

Are all writers trusted?

- No

Is public verifiability required?

- Yes

Ethereum
(Permissionless Blockchain)

- NO

Hyperledger
(Permissioned Blockchain)

- NO

Multichain
(Private Permissioned Blockchain)

- NO

Don't use Blockchain

- YES

Track the states of parking spots

- Multiple parties
  - Parking spots owners & renters

- Disintermediate

- Known parking spots owners
- Track the states of parking spots
- Multiple parties
  - Parking spots owners & renters
- Disintermediate
- Known parking spots owners
- Track the states of parking spots
- Multiple parties
  - Parking spots owners & renters
- **Disintermediate**
- Known parking spots owners
- Track the states of parking spots
- Multiple parties
  - Parking spots owners & renters
- Disintermediate
- Known parking spots owners
- Track the states of parking spots
- Multiple parties
  - Parking spots owners & renters
- Disintermediate
- **Known parking spots owners**
- Track the states of parking spots
- **Multiple parties**
  - Parking spots owners & renters
- **Disintermediate**
- Known parking spots owners

**Parameters**
- Do you need to store state?
- Are there multiple writers?
- Can you always use an online TTP?
- Are all writers known?
- Are all writers trusted?
- Is public verifiability required?

**Blockchain Options**
- **Ethereum** (Permissionless Blockchain)
- **Hyperledger** (Permissioned Blockchain)
- **Multichain** (Private Permissioned Blockchain)
- Don’t use Blockchain

---

34
Do you need to store state?

- NO

Are there multiple writers?

- NO

Can you always use an online TTP?

- YES

Are all writers known?

- NO

Are all writers trusted?

- NO

Is public verifiability required?

- YES

**Ethereum**
(Permissionless Blockchain)

- NO

**Hyperledger**
(Permissioned Blockchain)

- YES

**Multichain**
(Private Permissioned Blockchain)

- NO

**Don’t use Blockchain**

- YES

- Track the states of parking spots

- **Multiple parties**
  - Parking spots owners & renters

- Disintermediate

- Known parking spots owners
- Track the states of parking spots
- Multiple parties
  - Parking spots owners & renters
- Disintermediate
- Known parking spots owners
● **Track the states of parking spots**
● **Multiple parties**
  ○ Parking spots owners & renters
● **Disintermediate**
● **Known parking spots owners**
Blockchain-based parking app (dApp)

Requirements engineering, analysis and design