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 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?

- **NO**
  - NO
  - NO
  - NO
  - NO
  - NO

- **YES**
  - Are there multiple writers?
    - NO
    - NO
  - Can you always use an online TTP?
    - NO
    - NO
    - NO
    - NO
    - NO
  - Are all writers known?
    - NO
    - NO
    - NO
    - NO
    - NO
  - Are all writers trusted?
    - NO
    - NO
    - NO
    - NO
    - NO

- **YES**
  - Is public verifiability required?
    - YES
      - Ethereum (Permissionless Blockchain)
    - NO
      - 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 to store state?

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

- **NO**
  - *Don’t use Blockchain*

---

- **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?

Can you always use an online TTP?

Are all writers known?

Is public verifiability required?

• Coin management
  ○ Add, View, update, delete

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

• Other details

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?

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

Is public verifiability required?
Do you need a Blockchain?

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

[Weß 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?
    - **NO**
      - Can you always use an online TTP?
        - **NO**
          - Are all writers known?
            - **NO**
              - Is public verifiability required?
                - **YES**
                  - Hyperledger (Permissioned Blockchain)
                - **NO**
                  - Multichain (Private Permissioned Blockchain)
                - **YES**
                  - Don’t use Blockchain
            - **YES**
              - All writers trusted?
                - **YES**
                  - Ethereum (Permissionless Blockchain)
                - **NO**
                  - Hyperledger (Permissioned Blockchain)
        - **YES**
          - All writers trusted?
            - **YES**
              - Ethereum (Permissionless Blockchain)
            - **NO**
              - Multichain (Private Permissioned Blockchain)
    - **YES**
      - Multiple writers
        - **NO**
          - System should be more transparent
        - **YES**
          - Disintermediate

- **NO**
  - 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

**Flowchart**

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

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

- **NO**: 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**
**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?

- 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

- YES

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?  

- **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 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

---

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?

- Ethereum (Permissionless Blockchain)
- Hyperledger (Permissioned Blockchain)
- Multichain (Private Permissioned Blockchain)

Don’t use Blockchain
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

- Are you tracking the states of parking spots?
- Are there multiple writers?
- Can you always use an online TTP?
- Are all writers known?
- Are all writers trusted?
- Is public verifiability required?

- 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?
    - **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**
              - **YES**
                - **Don’t use Blockchain**
        - **YES**
          - **YES**
            - **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
- 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
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

Yes, choose:

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

No, choose:

- 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