Blockchain patterns and oracles
Lecture goals

● Blockchain patterns
● Blockchain oracles
  ○ Blockchain oracles types
    ■ Pull-based inbound
    ■ Push-based inbound
    ■ Pull-based outbound
    ■ Push-based outbound
Blockchain patterns

Blockchain patterns enable reusable solution and provide architectural guidance

- Patterns for interaction with external world
  - Oracles, legal and smart contact pair
- Data management patterns
  - Encrypting on-chain data, tokenization, state channel, off-chain data storage
- Security patterns
  - Multiple authorization, off-chain enabled dynamic authorization
  - X-confirmation
- Contract structural patterns
  - Registry contract, embedded permission, data contract, factory contract
  - Intensive execution
**Blockchain oracles**

- Smart contracts cannot make calls to access data outside the blockchain
- No native way for the blockchain to fetch external data.
- Blockchain oracles are software components
  - Allow communication between off-chain applications and blockchain applications
Blockchain oracles
Blockchain oracles types

- Pull-based inbound
- Push-based inbound
- Pull-based outbound
- Push-based outbound
Pull-based inbound

- Smart contract initiates the interaction
- Data flows from an off-chain application to the blockchain
- Off-chain component subscribes to events on the blockchain
  - Events are used by on-chain requesters to fetch information from outside the blockchain
    - Fetch the data and send a signed transaction containing the data to the requesting smart contract
- Such oracles can be used to verify a buyer’s creditworthiness once an order is made by the buyer
Pull-based inbound

[Diagram showing the interaction between Smart Contract, Bridge, and Off-Chain Application]

1. **EventSubscription**
   - **eventName**: "RequestForExchangeRate"

2. **Event**

3. **EventNotification**
   - **notificationPath**: "/requestExchangeRate"

4. **TransactionRequest**

5. **SendTransaction**
   - **privateKey**: "C:sers\user\repos\thesis\oracle\privkey2"
   - **smartContractFunctionName**: "updateExchangeRate"
Push-based inbound

- Initiator is an off-chain component
- Data flow is from an off-chain application to the blockchain
- Off-chain component is configured to query the status of an off-chain component and send data under certain conditions
  - The data is then translated into a blockchain transaction and sent on the blockchain
- Such oracles can be used to send the notification that a package has been delivered along with the parcel’s information
Push-based inbound
Pull-based outbound

- Initiator is an off-chain component
- Data flow is from the blockchain to an off-chain application
  - For example, a web application could query the status of the production of a specific good
Pull-based outbound

```
<SmartContract>
Smart contract
[abiPath = "C:\Users\levas\repos\thesis_oracle\lottery.abi",
chainId = 4,
contractAddress = "0x494536eF0C3efC3EaB336230740"]

<Oracle>
{caCertificate = "C:\Users\levas\repos\thesis_oracle\certs\oracle_certificate.pem",
generatedCodeDirectory = "C:\Users\levas\repos\thesis_oracle",
nodeUrl = "wss://rinkeby.infura.io/ws/v3/78d7341510ad4c84ad8211eb7ab10148",
oracleType = "pull-based outbound",
port = 3002,
serverCertificate = "C:\Users\levas\repos\thesis_oracle\certs\oracle_certificate.pem",
serverKey = "C:\Users\levas\repos\thesis_oracle\certs\oracle_key.pem"}

<OffChainApplication>
Off-Chain Application
{host = "localhost",
port = 3001}
```

```
1: «TransactionRequest»
2: «CallTransaction»
   {smartContractFunctionName = "getNumberOfRemainingTickets"}
3: «TransactionReply»
4: «TransactionReplyNotification»
```
Push-based outbound

- Initiator is an on-chain component
- Data flow is from the blockchain to an off-chain application
  - For example, a notification could be sent from a smart contract to a web application once an event listener has detected that a package has been delivered
Push-based outbound
Reading material

● Model-Driven Engineering of Blockchain Oracles

● Blockchain Oracles: A Framework for Blockchain-Based Applications
  ○ https://www.researchgate.net/publication/344079826_Blockchain_Oracles_A_Framework_for_Blockchain-Based_Applications

● Blockchain Oracles Explained

● What Is a Blockchain Oracle? What Is the Oracle Problem?
  ○ https://www.youtube.com/watch?v=ZJfkNzyO7-U
Lecture goals

- Blockchain patterns
- Blockchain oracles
  - Blockchain oracles types
    - Pull-based inbound
    - Push-based inbound
    - Pull-based outbound
    - Push-based outbound