BLOCKCHAIN TECHNOLOGY

Smart Contracts

Introduction

- This smart contract concept is not new
- With the advent of the blockchain
  - interest in this idea was revived
- is now an active area of research in the blockchain because of
  - reducing the cost of transactions
  - Simplifying complex contracts

Smart contract history

- first theorized in late 1990s
- almost 20 years later
  - potential and benefits are appreciated with the invention of Bitcoin and blockchain technology.
- Smart contracts are described as follows
  - an electronic transaction protocol that executes the terms of a contract.
  - general objectives are
    - to satisfy common contractual conditions such as
      - payment terms
      - Liens
      - Confidentiality
      - and even enforcement
    - To minimize exceptions
      - both malicious and accidental
    - To minimize the need for trusted intermediaries
  - Related economic goals include lowering
    - fraud loss
    - arbitrations
    - enforcement costs
    - Other transaction costs

Smart contract definition

- There is no consensus on a standard definition
- One definition is
  - A smart contract is a secure and unstoppable computer program representing an agreement that is automatically executable and enforceable
    - It is a computer program
    - it encompasses agreements between parties
      - in the form of business logic
    - It is automatically executed when certain conditions are met
    - It is enforceable
      - The code is law
      - all contractual terms are executed as defined and expected
        - even in the presence of adversaries
    - It is secure and unstoppable
      - fault-tolerant
      - executable in a reasonable amount of time

Smart contract definition

- Even though smart contracts are named smart
  - they are not really smart
    - they in fact only do what they have been programmed to do
    - they produce same output every time they are executed.
      - highly desirable deterministic nature
      - allow a smart contract to be run by any node on a network and achieve the same result
      - always produce the same results for a specific input
      - if results are inconsistent between nodes
        - then consensus will never be achieved

Smart contract definition

- language itself should be deterministic
    - Have no non-deterministic functions
        - which can produce different results on various nodes
    - E.g., various floating-point operations
        - can produce different results in different runtime environments

Smart contract definition

- In summary
  - a smart contract has the following four properties:
    - Automatically executable
    - Enforceable
    - Semantically sound
    - Secure and unstoppable
  - The first two are required as a minimum
  - the latter two may not be required in some scenarios
    - E.g., financial derivatives contract
      - does not perhaps need to be semantically sound and unstoppable
      - But should at least be automatically executable and enforceable at a fundamental level

Oracles

- smart contracts cannot access external data
    - might be required to control the execution of the business logic
        - E.g., the stock price of a security product that is
            - required by the contract to release the dividend payments.
- An Oracle is an interface
    - delivers data from an external source to smart contracts.

Oracles

- Oracles can deliver different types of data
  - weather reports
  - real-world news
  - corporate actions
  - data coming from IoT devices
- Oracles are trusted entities
  - use a secure channel to transfer data to a smart contract
  - capable of digitally signing the data
    - proving that the source of the data is authentic.

Oracles

- Smart contracts can subscribe to the Oracles
  - the smart contracts can either pull the data
  - or Oracles can push the data to the smart contracts
- Oracles should not be able to manipulate the data
  - must be able to provide authentic data.

Oracles

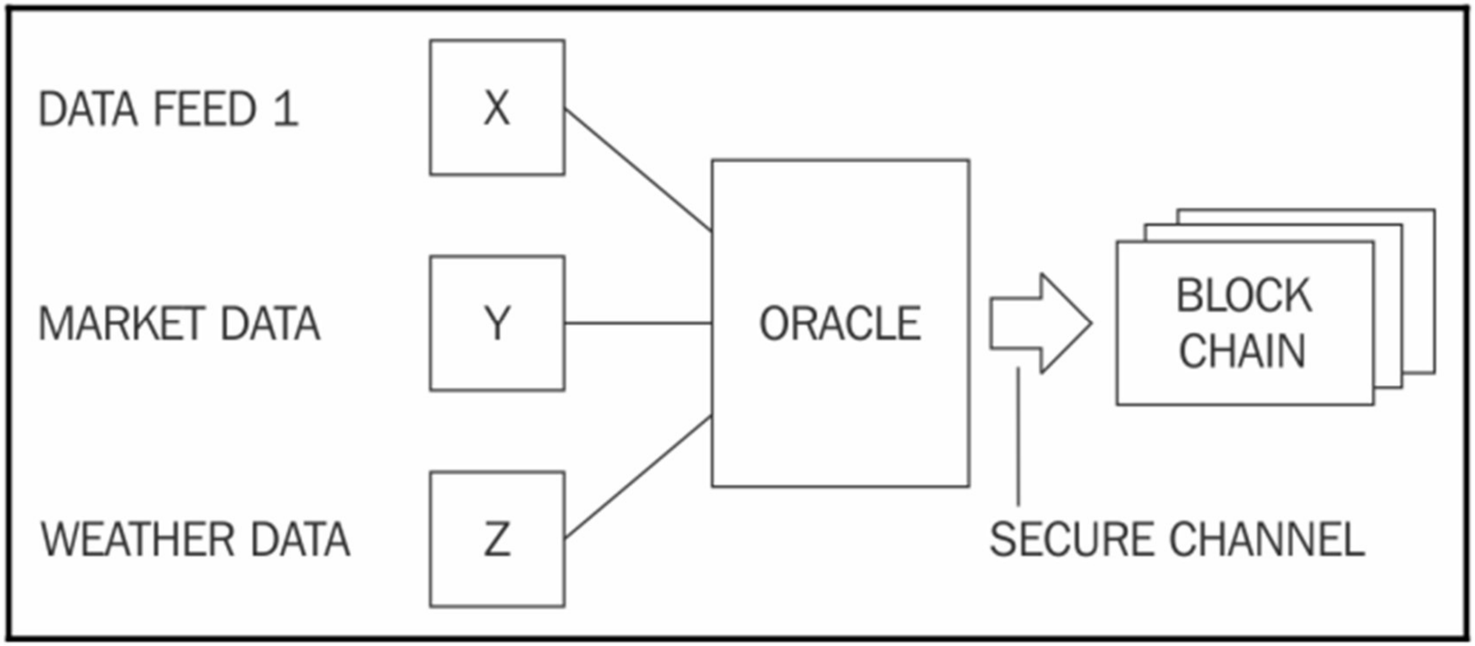
- The issue of trust
  - How do you trust a third party about the quality and authenticity of data they provide?
  - especially true in the financial world
    - market data must be accurate and reliable
- The issue of centralization
  - A large, reputable, trusted third party may be a good oracle
    - It will become a single point of failure

Oracles

- Decentralized Oracles
  - can be built based on some distributed mechanism
  - Oracles can find data from another blockchain
    - driven by distributed consensus
    - ensuring the authenticity of data
  - E.g., one institution running their private blockchain
    - can publish their data feed via an Oracle

Oracles

- Generic model of an Oracle and smart contract ecosystem



The DAO

- one of the highest crowdfunded projects
  - it started in April 2016
  - was a set of smart contracts to provide a platform for investment.
  - Was hacked due to a bug in the code
    - 50 million dollars was siphoned out of the DAO
    - resulted in a hard fork on Ethereum
      - to recover from the attack
  - The hard fork was against the notion of *code is law*
    - There was resistance against this hard fork
    - some miners decided to keep mining on the original chain
      - resulted in the creation of Ethereum Classic
        - where *the code is still the law*