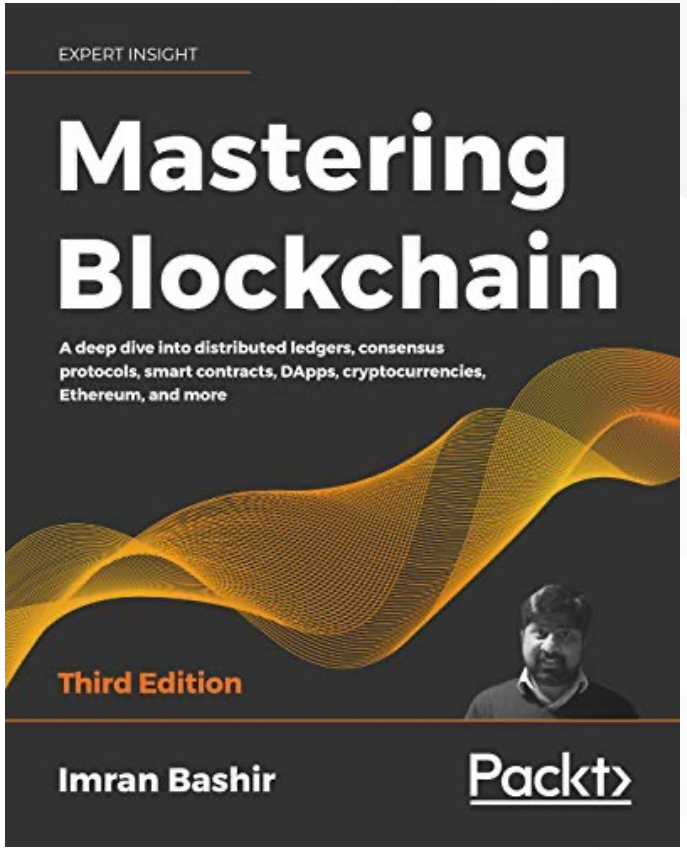
Mastering Blockchain

Third Edition

Chapter 10, Smart Contracts



Outline

- Ideas
- History
- Ricardian contracts
- Templates
- Oracles
- Types of oracles
- The DAO

Definition

"A smart contract is an electronic transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs."

Nick Szabo

Definition

A smart contract is a secure and unstoppable computer program representing an agreement that is automatically executable and enforceable.

- Secure
- Deterministic
- Semantically sound
- Unstoppable. Once executed, the smart contract cannot be halted and once deployed it usually cannot be changed.

Ricardian contracts

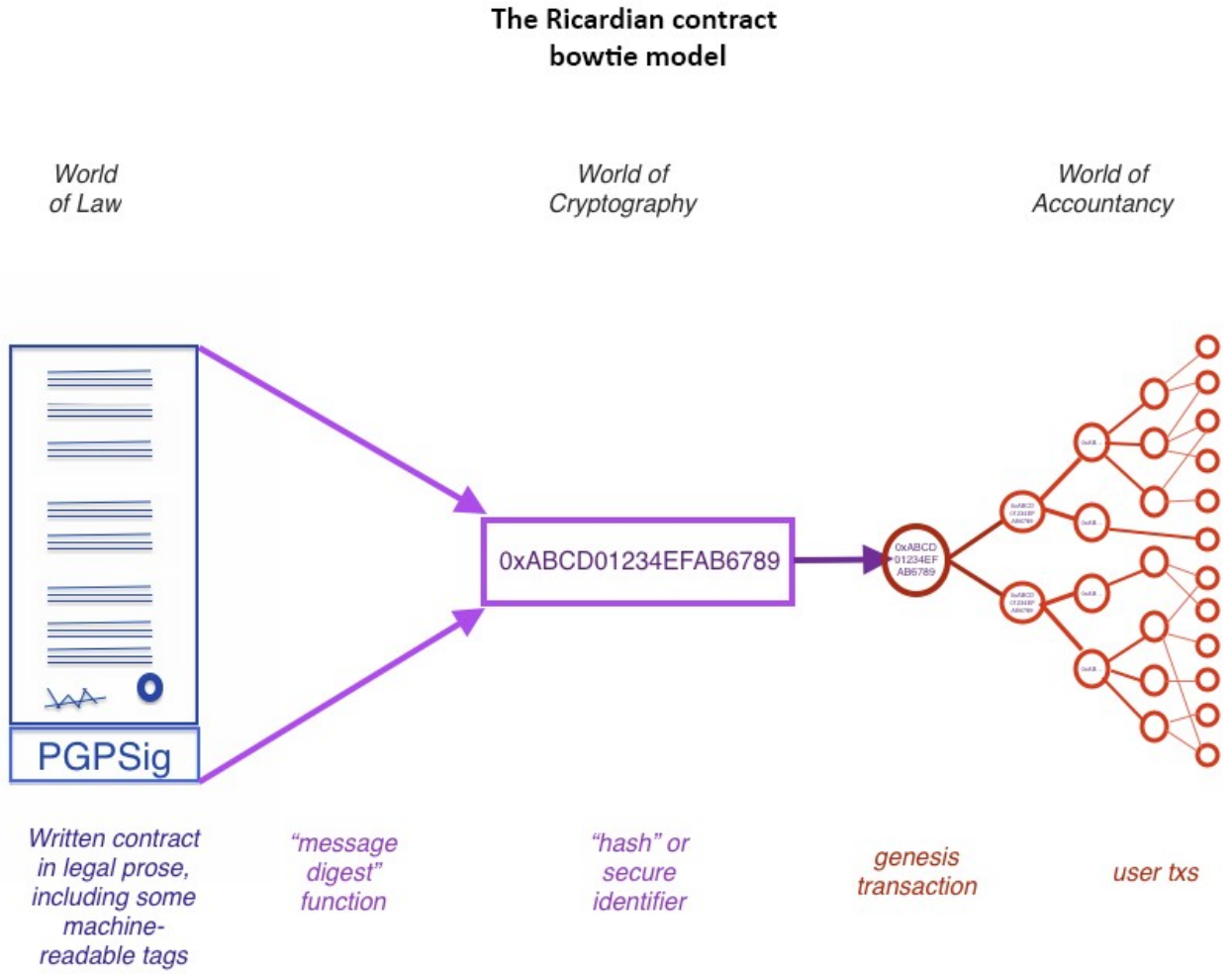
Ricardian contracts were introduced in *Financial Cryptography in 7 Layers*, by Ian Grigg, in the late 1990s.

- It is a contract offered by an issuer to holders
- It is a valuable right held by holders and managed by the issuer
- It can be easily read by people (like a contract on paper)
- It can be read by programs (parsable, like a database)
- It is digitally signed
- It carries the keys and server information
- It is allied with a unique and secure identifier

Ricardian contract model

Ricardian contracts can record a document as a legal contract, and securely link it with other IT systems.

- They use cryptographic hashes for identification
- They include human-readable legal prose, and machine-readable code!



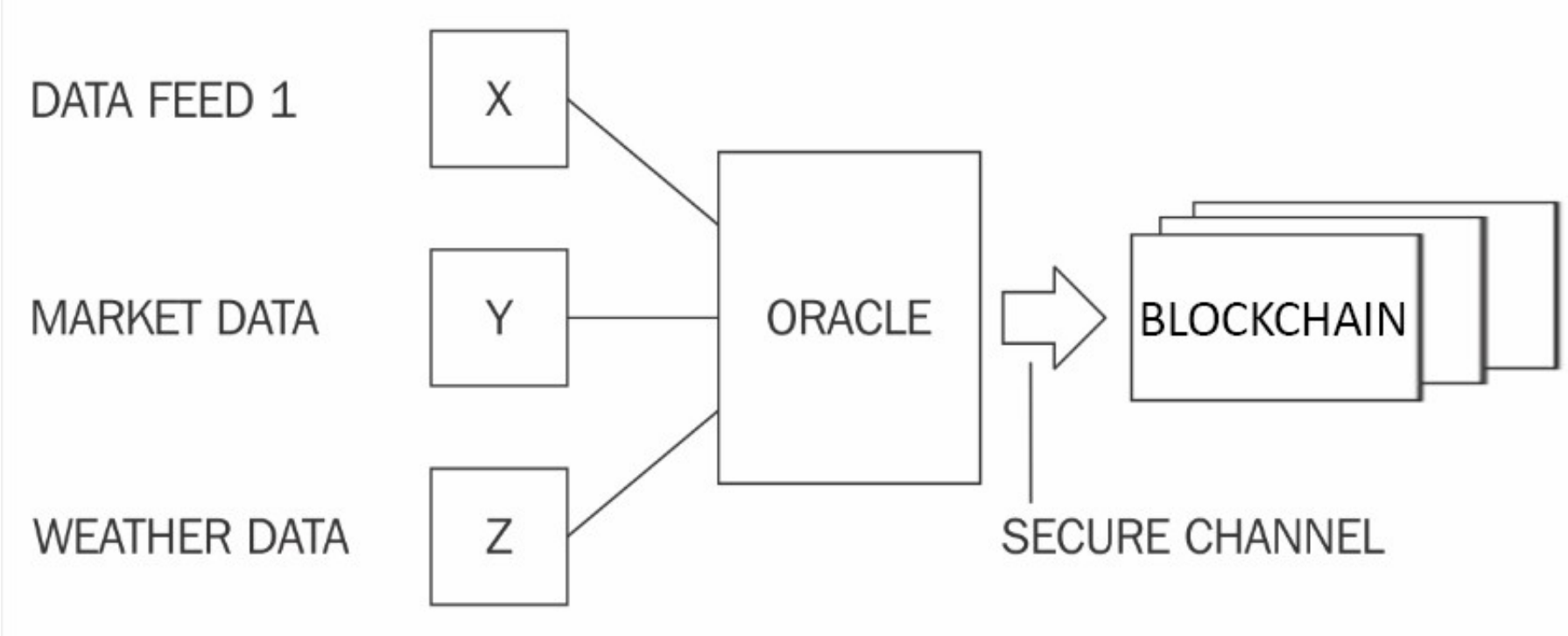
Smart contract templates

- A framework to support legal agreements for financial instruments
- Domain-Specific Languages (DSLs)
- Common Language for Augmented Contract Knowledge (CLACK)

Oracles

Oracles act as interface between the external world and the blockchain domain.

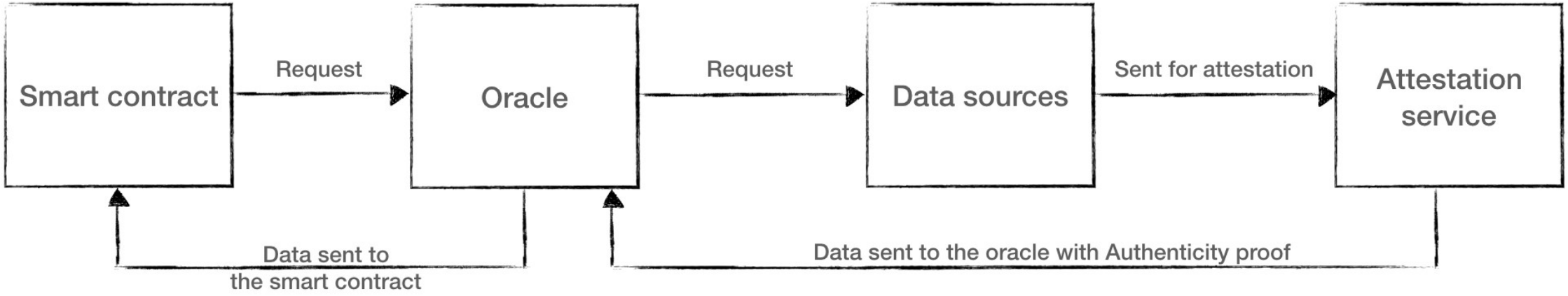
- An oracle usually takes data from the outside world, then feeds it securely to the blockchain
- In some cases, the process is implemented in reverse



Common use cases of smart contracts

Type of data	Examples	Use case
Market data	Live price feeds of financial instruments. Exchange rates, performance, pricing, and historic data of commodities, indices, equities, bonds, and currencies.	DApps related to financial services, for example, decentralized exchanges and **decentralized finance** (**DeFi**)
Political events	Election results	Prediction markets
Travel information	Flight schedules and delays	Insurance DApps
Weather information	Flooding, temperature, and rain data	Insurance DApps
Sports	Results of football, cricket, and rugby matches	Prediction markets
Telemetry	Hardware IoT devices, sensor data, vehicle location, and vehicle tracker data	Insurance DApps Vehicle fleet management DApps

Generic oracle data flow



Proofs of data integrity and authenticity in oracles

Several type of proof are used to authenticate the integrity of the data fed to the blockchain by oracles:

- Software and network-assisted proofs
- TLSNotary
- TLS-N based mechanism
- Hardware device-assisted proofs
- Android proof
- Ledger proof
- Trusted hardware-assisted proofs

Types of oracle

- Inbound oracles
- Software oracles
- Hardware oracles
- Computation oracles
- Aggregation-based oracles
- Crowd wisdom-driven oracles
- Decentralized oracles
- Smart oracles
- Outbound oracles

The DAO

The Decentralized Autonomous Organization (DAO), started in April 2016, was a smart contract written to provide a platform for investment. Due to a bug in the code, an equivalent of approximately 3.6 million ether (roughly 50 million US dollars) was siphoned out of the DAO into another account.

- Originally a platform for investment
- Contained a reentrancy bug
- Resulted in an Ethereum hard fork
- Raised questions regarding the *the code is law* theory

Exercise

- Analyze line 666 of the DAO and find reasons that why reentrancy was possible—use internet search and other sources of information as required

Summary

In this presentation, we considered a number of concepts related to smart contracts, including:

- History
- Ricardian contracts
- Templates
- Oracles
- The DAO
- An exercise to understand the DAO reentrancy bug